COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

9 juillet 2018
Strasbourg, France

T-CY(2017)10

Comité de la Convention sur la cybercriminalité (T-CY)

Groupe de travail sur la cyberintimidation et les autres formes de violence en ligne, en particulier contre les femmes et les enfants

Etude cartographique sur la cyberviolence

avec les recommandations adoptées par la T-CY le 9 juillet 2018

www.coe.int/cybercrime

Contenu

Contact

Alexander Seger
Secrétaire exécutif du Comité de la Convention sur la cybercriminalité (T-CY)
Direction générale des droits de l'homme et de l'État de droit
Conseil de l'Europe, Strasbourg, France
Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

1 Introduction

Les actes de violence à l'encontre d'individus commis au moyen ou facilités par les technologies de l'information et de la communication ("cyberviolence") sont devenus une préoccupation majeure pour les sociétés et les individus.

T-CY 16 (Strasbourg, novembre 2016) a donc décidé :

- De prendre note du ferme appui à la création d'un groupe de travail T-CY sur la cyberintimidation et les autres formes de violence en ligne, en particulier contre les femmes et les enfants - sur la base de l'article 1.1.j du Règlement intérieur de T-CY - et
- charger le Groupe d'étudier le sujet sous la forme d'un exercice de cartographie, comprenant des approches comparatives de la législation ainsi que la documentation des bonnes pratiques en vue de présenter des résultats intermédiaires à la 17e séance plénière et un rapport final à la 18e séance plénière de l'Assemblée T-CY.[1]

La 18e session plénière de novembre 2017 a ensuite pris une décision :

- Prolonger le mandat du Groupe de travail jusqu'au 31 juillet 2018 et demander au Groupe de soumettre un projet final de l'étude cartographique à T-CY 19 (juillet 2018) et de faciliter un atelier sur ce sujet à la Conférence Octopus en juillet 2018.

Alors que la cyberviolence peut viser n'importe quel individu ou groupe et peut impliquer un large éventail d'actes, cette étude cartographique se concentre en particulier sur les enfants et les femmes, qui sont souvent les victimes de la cyberviolence. L'expérience et les solutions concernant ces victimes devraient être applicables à d'autres catégories de victimes tout en tenant compte des spécificités de la violence contre les différentes catégories de victimes.[2]

La présente étude vise donc à :[3]

- cartographier les actes qui constituent la cyberviolence et tirer des conclusions sur les typologies et les concepts ;
- fournir des exemples d'expériences et de réponses nationales à de tels actes (y compris les politiques, les stratégies, la législation, les affaires et la jurisprudence) ;
- l'examen des réponses internationales au titre de la Convention de Budapest et d'autres traités (en particulier les Conventions d'Istanbul et de Lanzarote du Conseil de l'Europe) ;
- l'élaboration de recommandations quant à la marche à suivre.

En tant qu' « étude cartographique », le présent rapport ne vise pas à fournir une analyse complète et finale du phénomène de la cyberviolence et de ses réponses.

L'étude représente les conclusions du Groupe et a été prise en compte par la 19ème session plénière du T-CY le 9 juillet 2018. Le T-CY a adopté à cette occasion les « recommandations » et le « suivi » proposés dans les sections 4.2 et 4.3.

[1] Le groupe comprenait Markko KUNNAPU (Estonie), Erik PLANKEN (Pays-Bas), Gareth SANSOM (Canada), Cristina SCHULMAN (Roumanie), Eirik Tronnes HANSEN (Norvège), Branislav KADLECIK (Slovaquie) et Laura-Kate BERNSTEIN (Etats-Unis), et était soutenu par Betty SHAVE (Conseillère en Europe).
[2] Pour la terminologie relative à l'exploitation et aux abus sexuels concernant des enfants, voir les Lignes directrices de Luxembourg (Lignes directrices terminologiques pour la protection des enfants contre l'exploitation et les abus sexuels) adoptées par un groupe de travail interinstitutions à Luxembourg le 28 janvier 2016.)
http://luxembourgguidelines.org/fr/version-francaise/
[3] Une Partie à la Convention de Budapest n'est pas en adéquation avec la portée de l'étude.

Cette étude et son éventuel suivi peuvent également être considérés comme une contribution à l'Agenda 2030 des Nations Unies et aux Objectifs du développement durable (ODD), qui visent à « favoriser des sociétés pacifiques, justes et inclusives, exemptes de peur et de violence »[4].

2 Cartographie des phénomènes

2.1 Aperçu de la cyberviolence

2.1.1 Définition de la cyberviolence

En raison de l'ampleur potentielle des phénomènes et de la diversité des catégories et sous-catégories, déterminer l'objet de cet exercice de cartographie a été un défi permanent. Le Groupe de travail est finalement parvenu à un consensus sur l'utilisation du terme « cyberviolence » comme le terme le plus concis à utiliser tout au long de l'étude, en le définissant comme suit :

> La cyberviolence est l'utilisation de systèmes informatiques pour causer, faciliter ou menacer de causer à des personnes de la violence qui entraine ou est susceptible d'entrainer un préjudice ou des souffrances physiques, sexuelles, psychologiques ou économiques et peut comprendre l'exploitation de leur situation, de leurs caractéristiques ou de leur vulnérabilité.[5]

Les informations reçues des Parties donnent à penser que certains pays ont des lois qui traitent spécifiquement de formes particulières de cyberviolence. Bien que la cyberviolence existe depuis quelques années, ses formes spécifiques ne semblent pas avoir été identifiées et comprises que récemment. La plupart des pays s'efforcent de reconnaître les différentes facettes du problème et de les traiter dans leur droit interne.

Il est essentiel de rappeler que de nombreuses formes de cyberviolence sont déjà couvertes dans le droit national ou international par des dispositions relatives au « monde physique » et que les enquêtes n'auront peut-être pas à attendre l'adoption de nouvelles lois.

Par exemple, lorsque les ordinateurs sont utilisés pour provoquer ou faciliter la violence par la transmission de messages qui causent un préjudice psychologique, ou par la publicité pour meurtre, viol, enlèvement ou traite d'êtres humains, ces cas peuvent être poursuivis (en fonction de leurs faits) comme agression, violation de la vie privée, menace illégale, extorsion, sollicitation

---

[4] GDD 16 « Promouvoir des sociétés pacifiques et inclusives pour le développement durable, assurer l'accès à la justice pour tous et mettre en place des institutions efficaces, responsables et inclusives à tous les niveaux ». https://sustainabledevelopment.un.org/post2015/transformingourworld
https://www.coe.int/fr/web/un-agenda-2030/home

[5] Cette définition de travail est une adaptation du contexte « cyber » de la définition de la violence à l'égard des femmes de l'article 3 de la Convention d'Istanbul qui la définit :

> *comme une violation des droits de l'homme et une forme de discrimination à l'égard des femmes et désigne tous les actes de violence sexiste qui causent ou sont susceptibles de causer aux femmes un préjudice ou des souffrances physiques, sexuelles, psychologiques ou économiques, y compris la menace de tels actes, la contrainte ou la privation arbitraire de liberté, que ce soit en public ou dans la vie privée.*

De même, l'article 1 de la Convention interaméricaine sur la prévention, la sanction et l'élimination de la violence contre les femmes (Convention de Belém do Para) définit la violence contre les femmes comme suit :

> *tout acte ou comportement, fondé sur le sexe, qui cause la mort ou un préjudice ou des souffrances physiques, sexuelles ou psychologiques aux femmes, que ce soit dans la sphère publique ou privée.*

Les Nations Unies fournissent également une définition complète de la violence à l'égard des femmes :

> *Tout acte de violence sexiste qui cause ou est susceptible de causer aux femmes un préjudice ou des souffrances physiques, sexuelles ou psychologiques, y compris la menace de tels actes, la contrainte ou la privation arbitraire de liberté, que ce soit en public ou dans la vie privée.*

http://www.un.org/womenwatch/daw/vaw/v-overview.htm
Toutes ces définitions ont en commun le fait que la « violence » ne se limite pas aux dommages corporels.
Les membres du Groupe de travail reconnaissent que cette définition de travail est assez large et qu'elle doit encore mûrir. D'autre part, tout crime peut avoir un élément « cyber » qui peut changer la nature et la portée du crime.

de viol ou meurtre, distribution illégale de contenus (comme des photographies), violence domestique, etc.

En outre, étant donné la dépendance à l'égard des systèmes informatiques - y compris la dépendance psychologique, physique et économique - certains types de cybercriminalité (accès illégal à des données personnelles intimes, destruction de données, etc.) peuvent être considérés comme des actes de cyberviolence.

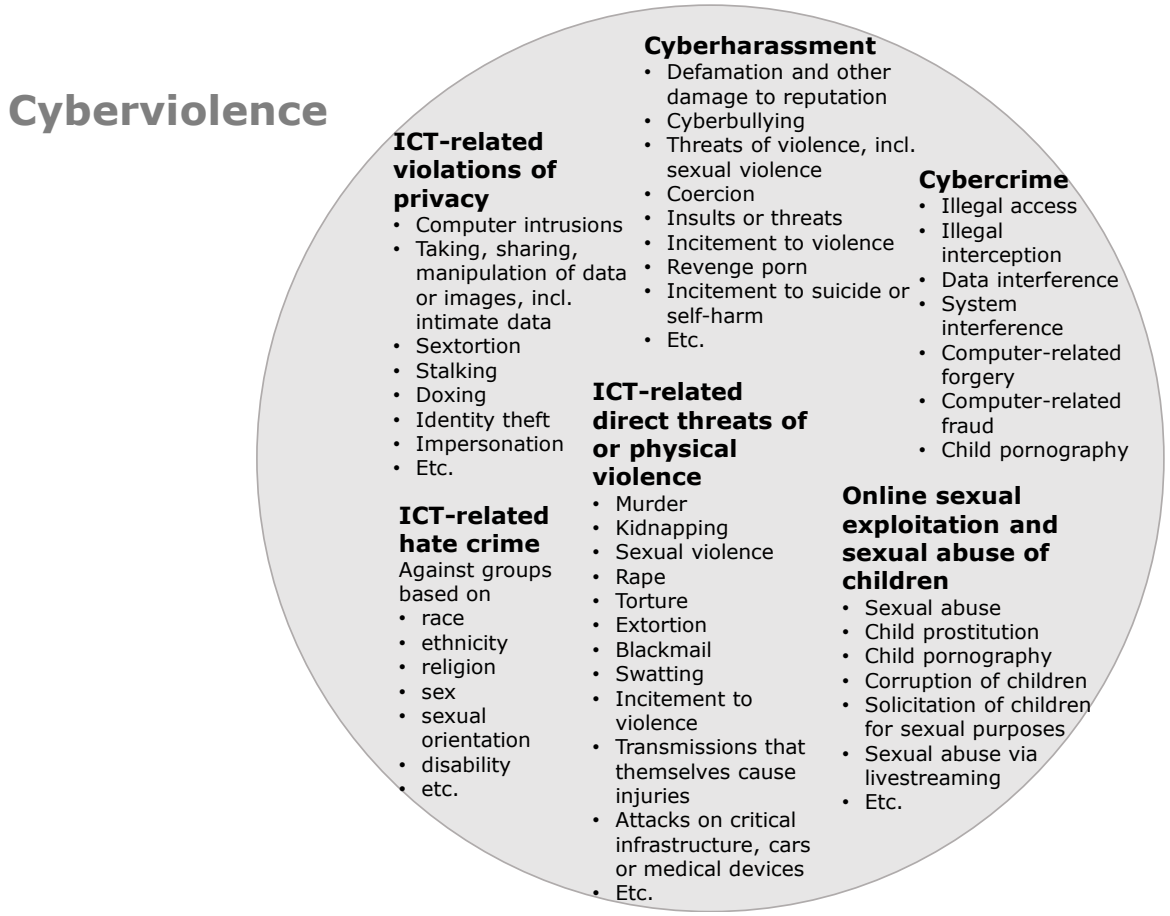
Les lois sur la cybercriminalité peuvent notamment s'appliquer lorsque des actes de violence tels que des blessures ou la mort sont commis, par exemple, par des attaques informatiques contre des infrastructures essentielles ou des dispositifs médicaux.

2.1.2 Types de cyberviolence

Dans la pratique, les actes de cyberviolence peuvent impliquer différents types de harcèlement, de violation de la vie privée, d'abus sexuel et d'exploitation sexuelle et d'infractions de préjugés contre des groupes sociaux ou des communautés. La cyberviolence peut également impliquer des menaces directes ou des violences physiques, ainsi que différentes formes de cybercriminalité.

Il n'existe pas encore de lexique ou de typologie stable des infractions considérées comme de la cyberviolence, et de nombreux exemples de types de cyberviolence sont interdépendants ou se recoupent ou consistent en une combinaison d'actes.

Toutes les formes ou tous les cas de cyberviolence ne sont pas aussi graves et ne nécessitent pas nécessairement une solution pénale, mais ils peuvent être traités par une approche progressive et une combinaison de mesures préventives, éducatives, protectrices et autres.



2.1.2.1 Cyberharcèlement

Le cyberharcèlement est peut-être la forme la plus large de cyberviolence. Il implique un comportement persistant et répété ciblant une personne en particulier qui est conçu pour causer une détresse émotionnelle grave et souvent la peur d'un préjudice physique.

Le cyberharcèlement est souvent le résultat d'une « tempête d'abus ». Les harceleurs terrorisent les victimes en menaçant de recourir à la violence. Les contrevenants affichent des faussetés diffamatoires pour causer de l'embarras à la victime ou pire parmi leurs amis, leur famille ou leurs collègues de travail. Les délinquants se font passer pour des victimes dans des publicités en ligne et laissent entendre - à tort - que leurs victimes s'intéressent aux relations sexuelles avec des étrangers. Parfois, les harceleurs manipulent les moteurs de recherche pour assurer la proéminence des mensonges dans la recherche des noms des victimes. Les auteurs de harcèlement portent atteinte à la vie privée des victimes en affichant des renseignements de nature délicate, comme des images de nus ou des numéros d'identification nationaux. Les harceleurs peuvent aussi utiliser la technologie pour mettre les gens hors ligne[6]. Dans le discours populaire, le cyberharcèlement peut être décrit comme étant lié à la « vengeance pornographique » ou à la « sextorsion ».

Le cyberharcèlement vise souvent les femmes et les filles et est appelé « cyberviolence contre les femmes et les filles » (GTVFAC ou GTVFAC) :

- Courriels ou autres messages sexuellement explicites non désirés ;
- Avancées offensives dans les médias sociaux et autres plateformes ;
- Menaces de violence physique ou sexuelle ;
- Le discours haineux renvoie à un langage qui dénigre, insulte, menace ou cible une personne en fonction de son identité (sexe) ou d'autres traits (comme l'orientation sexuelle ou un handicap).[7]

Le cyberharcèlement implique donc toute une série de comportements, comme par exemple la « cyberintimidation » et la « vengeance pornographique ».

2.1.2.1.1 Cyberintimidation

La cyberintimidation est une forme de cyberharcèlement qui tend à être associée à des victimes mineurs, souvent d'âge secondaire, alors que des phénomènes tels que la cyberharcèlement, la sextorsion ou la « pornographie de vengeance » sont plus susceptibles d'être associés aux adultes ou aux jeunes adultes. Les frontières entre ces deux termes ne sont pas distinctes et il n'existe pas, pour le moment, d'accord commun quant à l'utilisation de ces termes. Toutes les formes de cyberintimidation ne constituent pas nécessairement une infraction pénale.

La littérature identifie différents types de cyberintimidation qui incluent le cyberharcèlement, le dénigrement, la participation à des groupes d'exclusion/de ragots, la falsification d'identité pour afficher du contenu en ligne/du contenu injurieux, le harcèlement, l'usurpation d'identité, la "sortie", le phishing, le "sexting" et la tricker[8]. Comme l'ont fait remarquer certains auteurs[9], la cyberintimidation peut être considérée comme le parapluie de nombreuses activités d'intimidation

[6] Voir CITRON, DANIELLE K. *Addressing Cyber Harassment : Aperçu des crimes motivés par la haine dans le cyberespace*. University of Maryland Francis King Carey School of Law, document de recherche sur les études juridiques, no 2017-9, 2.
Voir aussi "The Disturbing Rise of Cyberattacks against Abortion Clinics" dans WIRED (10 mai 2017) https://www.wired.com/story/cyberattacks-against-abortion-clinics/
[7] https://eige.europa.eu/fr/in-brief
[8] Voir NOTAR, CHARLES E. ; PADGETT, SHARON ; RODEN, JESSICA. *Cyberintimidation : Ressources pour l'intervention et la prévention*. Universal Journal of Educational Research 1(3) : 133-145, 2013.
[9] Voir EL ASAM, AIMAN ; SAMARA, MUTHANNA. *La cyberintimidation et la loi : Un examen des défis psychologiques et juridiques*. Computers in Human Behavior 65 (2016) 127-141.

en ligne, dont certaines sont plus graves que d'autres et ont entraîné des manipulations sexuelles, la création et la distribution non consensuelles d'images ou de vidéos intimes, des actes d'extorsion, d'automutilation et du suicide.[10] C'est pourquoi, du point de vue des enquêtes et des poursuites criminelles, il est essentiel de faire la distinction entre les différents types de cyberintimidation. Il est également important de faire la distinction entre les différents rôles que jouent les individus dans un acte de cyberintimidation donné.

La cyberintimidation est définie sur le site Internet « Droits de l'enfant » du Conseil de l'Europe[11] comme l'utilisation des technologies électroniques pour intimider une autre personne sur Internet. Elle prend différentes formes. Parmi les exemples de cyberintimidation sont inclus les messages textuels ou les courriels désagréables, les rumeurs envoyées par courriel ou affichées sur des sites de réseautage social et les photos, vidéos ou sites Web embarrassants. La cyberintimidation implique généralement une série soutenue de tels messages, qu'ils soient orchestrés par une seule personne ou un groupe de pairs, et l'impact cumulatif peut être très dévastateur.

Différents auteurs ont donné des définitions variées de la cyberintimidation qui peut être considérée au sens large comme « tout comportement accompli par des individus ou des groupes au moyen de médias électroniques ou numériques qui communiquent de façon répétée des messages hostiles ou agressifs visant à nuire ou à gêner les autres ».[12]

Compte tenu du nombre croissant de victimes parmi les jeunes, mais aussi parmi les adultes - et étant donné que la cyberintimidation dans des cas extrêmes peut conduire à des suicides[13] - on assiste à une augmentation des recherches et des réponses réglementaires à cette forme de cyberviolence.

Parmi les victimes de cyberintimidation figurent des journalistes. Une récente étude du Conseil de l'Europe sur les « journalistes sous pression »[14] a montré que les journalistes de plus de la moitié des 47 Etats membres ont été victimes de cyberintimidation au cours des trois dernières années. La cyberintimidation a donc également un impact sur la liberté d'expression.

---

[10] Un exemple récent de cyberviolence est le défi "Blue Whale", qui s'articule autour d'un jeu vidéo où les participants reçoivent des points. Les enfants s'abonnent sur une page web afin d'être contactés par un « curateur », qui établira 50 tâches qui devront être accomplies dans les 50 jours suivants. Ces tâches comprennent de nombreuses activités, telles que regarder des vidéos au contenu extrêmement violent, ou s'automutiler dans des situations particulièrement dangereuses (par exemple sur le toit d'un bâtiment ou à proximité de voies ferrées ou d'autoroutes), mais aussi se blesser avec des objets tranchants. La dernière tâche est de se suicider. Le défi du "Blue Whale" semble être semblable au « grooming » ou « sollicitations sexuelles » (voir ci-dessous) ; cependant, le « grooming » est généralement associé en droit criminel à l'activité sexuelle et le "Blue Whale" est axé sur la « coupe » et l'automutilation.

[11] Voir http://www.coe.int/fr/web/children/bullying (lien vérifié pour la dernière fois le 12 septembre 2019).

[12] Voir TOKUNAGA, Robert S. *Te suivre à la maison après l'école : Un examen critique et une synthèse de la recherche sur la victimisation par cyberintimidation*. Computers in Human Behavior, 26(3), 278.
Pour d'autres définitions, voir :
Voir VAN LEEUWEN, J.C. Literature Review on the research on cyberbullying definitions. Universiteit Twente. (2012). MOORE, Michael J. ; NAKANO Tadashi ; ENOMOTO Akihiro ; SUDA Tatsuya. *Anonymat et rôles associés aux messages agressifs dans un forum en ligne*. Computers in Human Behavior (2012).
JUVONEN, Jaana ; GROSS Elisheva F. *Extending the School Grounds?-Bullying Experience in Cyberspace*. Journal of School Health. Vol. 78(9). (2008), 496-505.
BESLEY, Bill. Publié sur http://www.cyberbullying.ca/ (lien vérifié pour la dernière fois le 12 septembre 2019).
SMITH, Peter K. ; MAHDAVI Jess ; CARVALHO Manuel ; FISHER Sonja ; RUSSELL Shanette ; TIPPETT Neil. *Cyberintimidation : sa nature et son impact sur les élèves du secondaire*. The Journal of Child Psychology and Psychiatry. Vol. 49(4). (2008), 376-385.
KOWALSKI, Robin M. ; LIMBER, Susan P. *Electronic Bullying Among Middle School Students*. Journal of Adolescent Health 41 (2007) S22-S30.
ERDUR-BAKER, Özgür. *La cyberintimidation et sa corrélation avec l'intimidation traditionnelle, le genre et l'utilisation fréquente et risquée des outils de communication par Internet.* Nouveaux médias et société. Vol. 12(1). (2009), 109-125.

[13] Pour une vue d'ensemble de quelques cas très médiatisés, voir *The Top Six Unforgettable CyberBullying Cases Ever* publié sur https://nobullying.com/six-unforgettable-cyber-bullying-cases/ (lien consulté pour la dernière fois le 12 septembre 2019).

[14] Clark, Marilyn/Grech, Anna (2017) : Des journalistes sous pression. L'ingérence injustifiée, la peur et l'autocensure en Europe. Editions du Conseil de l'Europe. Strasbourg.

La documentation associe souvent la cyberintimidation aux médias sociaux comme YouTube, Facebook, Tumblr, Twitter, Instagram, Snap Chat, WhatsApp et les forums de discussion. Grâce à ces médias, il est facile d'envoyer des messages menaçants, du matériel audiovisuel offensant ou des "insultes" en ligne aux gens. Il existe de nombreux exemples de ce type de comportement : le toilettage, le sexting, le trolling et le piratage d'identité.

La littérature scientifique identifie quatre éléments qui caractérisent la cyberintimidation et la distingue des formes inoffensives de comportement en ligne telles que la cyber-guérison ou la cyberdiscussion[15]. Ces critères sont les suivants :

- Intention de blesser - L'auteur a l'intention de blesser la victime en lui causant intentionnellement une perte de réputation dans la société, et/ou au travail, et/ou en détruisant ses relations familiales, ou en causant d'autres dommages**.**

- Déséquilibre de pouvoir - Dans le monde physique, l'agresseur a généralement une interaction sociale avec la victime dans laquelle l'agresseur est plus fort physiquement et/ou mentalement, soit par sa taille réelle, ses prouesses physiques ou son estime sociale. Généralement, dans le cas de la cyberintimidation, un déséquilibre de pouvoir se produit soit à cause de la pression exercée par les pairs, ce qui entraîne l'ostracisme social et l'isolement (dans une forme du phénomène), soit à cause d'un auteur anonyme (dans une autre forme du phénomène). Les deux formes amplifient le déséquilibre du poseur en raison de la grande portée des messages sur les médias sociaux, ainsi que par le fait que les messages affichés sont difficiles à retirer complètement d'Internet. Internet permet aux gens - y compris ceux qui se connaissent en personne - de faire ou de dire en ligne des choses qu'ils ne feraient ou ne diraient jamais en contact direct. C'est ce qu'on appelle l' « effet de désinhibition » des médias numériques.

- Comportement récurrent et processus continu dans lequel la victime subit des abus répétés - Cela peut être pris littéralement en affichant des messages consécutifs ou découler du fait que les messages affichés peuvent être partagés, réaffichés et peuvent demeurer en ligne indéfiniment.

- Distribution non consensuelle d'images intimes - Les auteurs de ce type d'infraction ciblent souvent les jeunes et les femmes adultes, mais aussi les minorités et d'autres groupes vulnérables. En fait, si, d'une part, la disponibilité de plusieurs dispositifs capables de créer et d'échanger des images intimes a donné naissance à un marché émergeant de contenus pornographiques générés par les utilisateurs, que certains ont considéré comme habilitants[16]. D'autre part, la production et l'échange d'images sexuellement explicites peuvent être utilisés pour des activités criminelles, telles que le harcèlement criminel en ligne ou le cyberharcèlement, la sextorsion, le « porno de vengeance », le bavardage sexuel[17] et la manipulation, qui entrent dans la catégorie générale du harcèlement sexuel et qui sont principalement destinées aux femmes et aux jeunes filles.

[15] Les cyber-guérisons ou cyber-arguments font référence au comportement d'envoyer des messages qui ne sont pas destinés à nuire à une autre personne, qui ne sont pas nécessairement répétitifs et qui sont exécutés dans le cadre d'une relation de pouvoir égal.
[16] Voir PAASONEN, Sussanna. Les *travaux de l'amour : netporn, le Web 2.0 et les sens de l'amateurisme*. Nouveaux médias et société 12(8) 1297-1312.
[17] La discussion sexuelle peut être définie comme "[...] l'échange occasionnel d'opinions vernaculaires sur les croyances, les rumeurs et le comportement sexuels, menées de manière synchrone ou asynchrone ". Dans le cas du chat sexuel sur Internet, la communication peut se faire dans un environnement surveillé ou non surveillé défini par le webmaster. Voir ERNI, John Nguyet. *Sexe/Texte : Internet Sex Chatting et "Vernacular Masculinity" à Hong Kong*. International Proceedings of Economics Development and Research, Vol. 44, 56-60.

2.1.2.1.2 « Vengeance pornographique »[18]

Le terme « vengeance pornographique » est un terme utilisé dans le discours populaire qui met l'accent sur la représentation sexuellement explicite d'une ou de plusieurs personnes et qui est distribué sans le consentement du sujet. Le phénomène implique principalement un partenaire dans une relation intime qui diffuse le matériel dans le but d'humilier ou d'intimider la victime. Le phénomène, apparu dès les années 1980 (fait régulièrement l'objet d'articles dans le magazine *Hustler*), était lié à la « pornographie amateur », avant de se transformer en vidéos sexuellement explicites diffusées sur Internet (comme l'agrégateur de pornographie amateur Xtube, en 2008). La[19] « vengeance pornographique » est un crime reconnu par plusieurs réglementations locales et nationales et qui a donné lieu à des poursuites civiles et pénales dans différents pays, mais pas toujours de la même manière. Une formulation juridique criminalise la divulgation, la distribution, la diffusion ou la promotion illégale (c'est-à-dire non consensuelle) d'images ou de vidéos intimes.

Aux États-Unis, 35 États, ainsi que le district de Columbia ont adopté des lois poursuivant les crimes de vengeance pornographique,[20] tandis qu'en Europe et dans d'autres pays, la situation est plus fragmentée, ou moins réglementée.

Le Canada a modifié son Code criminel (article 162.1) en mars 2014 pour interdire la distribution non consensuelle d'images intimes (le Code est entré en vigueur en mars 2015). Une disposition connexe (article 162.2, modifié en 2015) habilite le tribunal à ordonner le retrait d'images intimes d'Internet ; autorise le tribunal à ordonner la confiscation de l'ordinateur, du téléphone cellulaire ou de tout autre dispositif utilisé pour commettre l'infraction ; prévoit le remboursement aux victimes des frais engagés pour retirer l'image intime sur Internet ou ailleurs ; et autorise le tribunal à rendre une ordonnance pour empêcher quiconque de diffuser les images intimes.

En Allemagne, en mai 2014, un tribunal a statué que les photographies intimes des partenaires devraient être supprimées si un partenaire le demande. La décision du tribunal régional supérieur allemand de Coblence fait suite au refus d'un homme divorcé de supprimer les images érotiques de son ex-épouse après leur séparation. Il a été poursuivi en justice par son ex-femme, qui a gagné son procès et a vu les photos effacées.[21]

En France, l'article 67 de la loi n° 2016-1321 du 7 Octobre 2016, dite loi « pour une République numérique » dispose :

> Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende. Est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images

[18] Il n'est pas recommandé d'utiliser ce terme dans le contexte de l'exploitation et de l'abus sexuels des enfants.
http://luxembourgguidelines.org/fr/version-francaise/
L'expression "abus sexuel fondé sur l'image" peut être utilisée comme alternative.
[19] En 2010, le site *IsAnyoneUp* a été lancé : il fournit souvent les informations d'identification du sujet dans les vidéos. Le propriétaire du site, Hunter Moore, a plaidé coupable de vol d'identité et de piratage informatique en 2015. Kevin Bollaert, qui dirigeait le site de vengeance pornographique *UGotPosted*, a été inculpé aux États-Unis de 31 chefs d'accusation, y compris d'extorsion et de vol d'identité, et condamné en 2015 à 18 ans de prison. En 2014, une décision rendue dans l'Ohio contre lui a accordé des dommages-intérêts de 385 000 $ au nom d'un mineur représenté sur les photos. D'autres affaires ont fait l'objet d'accusations au Royaume-Uni ces dernières années.
[20] https://www.cybercivilrights.org/revenge-porn-laws/
[21] https://www.thelocal.de/20140522/court-forces-ex-lovers-to-delete-sexy-photos

> présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1.[22]

En 2015, le Royaume-Uni a modifié la loi de 2015 sur la justice pénale et les tribunaux, y compris en ce qui concerne les « infractions impliquant l'intention de causer de la détresse » le crime de « divulgation de photographies et de films sexuels privés dans l'intention de causer de la détresse. »[23]

2.1.2.2 Violations de la vie privée liées aux TIC

De nombreuses formes de cyberviolence représentent ou sont liées à une violation de la vie privée des victimes.[24] Il peut s'agir d'intrusions informatiques pour obtenir, voler, révéler ou manipuler des données intimes, de la recherche et de la diffusion de données personnelles (" doxing ") ou d'actes tels que le « cyberharcèlement » ou le « sextortion/vengeance pornographique ».

2.1.2.2.1 Cyberharcèlement

Cyberharcèlement « [...] désigne le harcèlement criminel sous forme électronique. Avec l'anonymat, la facilité et l'efficacité d'Internet, le cyberharcèlement peut se produire de multiples façons. Les cyberharceleurs peuvent utiliser des renseignements personnels sur la victime pour la menacer ou l'intimider. Les cyberharceleurs peuvent également envoyer des courriels non désirés et répétitifs, ou des messages instantanés qui peuvent être de nature hostile et menaçante. Les cyberharceleurs peuvent également usurper l'identité de leurs victimes en ligne en volant les informations de connexion d'un compte de messagerie ou d'une page de réseautage social et en publiant des messages sur les pages d'autres pairs ». [25]

« Le harcèlement criminel comprend un ensemble de comportements répétés et intrusifs - comme le fait de suivre, de harceler et de menacer - qui font peur aux victimes. Ces[26] dernières années, ce phénomène a de plus en plus impliqué l'utilisation de technologies mobiles (comme les smartphones) ainsi que d'ordinateurs, d'ordinateurs portables, de tablettes et d'appareils photo numériques. Ce type de harcèlement prend principalement la forme d'hommes qui victimisent les femmes :

> Contrairement aux idées fausses répandues, la recherche montre que la majorité du harcèlement criminel est perpétré non pas par des étrangers ou des connaissances, mais par des partenaires intimes ou des ex-partenaires... Les faits démontrent que les hommes sont les principaux auteurs de harcèlement criminel par un partenaire intime, en Australie et à l'étranger..... Les études internationales montrent que les femmes sont plus susceptibles d'être harcelées que les hommes... et qu'elles sont plus susceptibles de ressentir de la peur en raison du harcèlement criminel.[27]

---

[22] https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=376F4C0A93A89EF3C437726AEDC9F209.tplgfr26s_1?idArticle=JORFARTI000033203291&cidTexte=JORFTEXT000033202746&dateTexte=29990101&categorieLien=id

[23] http://www.legislation.gov.uk/ukpga/2015/2/section/33

[24] Pour faciliter la localisation des personnes, voir par exemple https://www.wired.com/story/track-location-with-mobile-ads-1000-dollars-study/

[25] Voir MARCUM, CATHERINE D. ; HIGGINS, GEORGE E. ; RICKETTS, MELISSA L., *Juveniles and Cyber Stalking in the United States : An Analysis of Theoretical Predictors of Patterns of Online Perpetration*. International Journal of Cyber Criminology, vol. 8, numéro 1, p. 48.

[26] WOODLOCK, Delanie (2016) : *The Abuse of Technology in Domestic Violence and Stalking*. Violence à l'égard des femmes. Volume : 23 publication : 5, page(s) : 584-602 http://journals.sagepub.com/doi/full/10.1177/1077801216646277 (lien vérifié pour la dernière fois le 12 septembre 2019)

[27] Woodlock 2016 : 584-585

Les recherches indiquent que le cyberharcèlement par des partenaires intimes se produit souvent dans le contexte de la violence familiale et constitue une forme de *contrôle coercitif*[28]. Le harcèlement par des partenaires intimes peut être persistant et dangereux. Woodlock cite une enquête nationale américaine qui a révélé que « les cas impliquant des partenaires intimes duraient en moyenne 2,2 ans, comparativement à 1,1 an pour le harcèlement criminel par des tiers » et qui a été fortement associée aux homicides et aux tentatives d'homicide. Les TIC sont utilisées non seulement pour garder la victime sous surveillance (caméras numériques cachées, suivi GPS des véhicules), mais aussi pour le harcèlement et le contrôle par le biais de courriels persistants et de textos constants (SMS). Les comportements qui, dans d'autres contextes, sont menés de façon consensuelle pour le plaisir, comme le « sexting », sont utilisés de façon coercitive et non consensuelle pour contrôler, harceler ou humilier des partenaires intimes qui se livrent au cyberharcèlement.[29]

2.1.2.2.2 Sextorsion

La sextorsion est un terme utilisé dans le discours populaire qui englobe les activités qui (a) impliquent une manipulation ou une coercition pour exécuter des activités sexuelles au profit de l'agresseur et/ou pour créer des images sexuellement explicites de la victime, et (b) le crime traditionnel d'extorsion. Bien que le crime puisse inclure la menace de diffuser de telles images ou vidéos une fois qu'elles ont été créées, il est tout aussi courant que la coercition puisse impliquer la menace de blesser la famille ou les amis de la victime si une activité sexuelle n'est pas entreprise et enregistrée ou transmise à l'agresseur. La motivation de l'agresseur peut aussi être la vengeance, l'humiliation ou le gain monétaire. Elle s'effectue souvent à distance sur des réseaux informatiques et peut impliquer l'enregistrement d'images ou la diffusion vidéo en direct (c.-à-d. à l'aide d'une caméra Web). Les auteurs sont souvent des partenaires romantiques ou sexuels actuels, anciens ou potentiels.[30] Il existe cependant des cas de sextorsion où l'auteur est un étranger et un agresseur en série avec des victimes dans des dizaines de pays. Les délinquants utilisent souvent une variété de compétences en informatique, y compris le piratage informatique, la création de fausses identités multiples sur des sites de médias sociaux, l'interception de communications privées, etc. cet égard, la sextorsion fait partie des formes les plus graves de cyberintimidation et a également été un élément de certaines formes de cyberharcèlement. La « sextorsion » implique souvent la distribution non consensuelle d'images intimes, même si cette distribution se fait uniquement entre le délinquant et la victime, plutôt qu'une large diffusion.

[28] Woodlock (2016 : 585) déclare : « Le contrôle coercitif est un cadre théorique qui englobe la violence physique qui se produit dans la violence familiale, mais qui comprend aussi des tactiques qui ne sont pas traditionnellement considérées comme des formes graves de violence. Ces tactiques comprennent des stratégies de contrôle et d'intimidation, comme l'isolement, la surveillance, les menaces de violence, la microgestion des activités quotidiennes (p. ex., la réglementation des douches et des repas) et l'humiliation (Stark 2007). La théorie du contrôle coercitif englobe également les effets de ces tactiques sur les victimes. Stark (2012) croit que ces effets ont plus en commun avec les expériences des otages et des victimes d'enlèvements que des victimes d'agressions conventionnelles. Stark reconnaît que même si les femmes peuvent être violentes dans les relations intimes, les hommes sont les principaux auteurs du contrôle coercitif parce qu'il s'agit d'une forme de violence ancrée dans l'inégalité systémique, qui confère aux hommes un privilège fondé sur le sexe. Stark considère ce privilège fondé sur le sexe comme l'essence même du contrôle coercitif, où les délinquants de sexe masculin « exploitent les inégalités sexuelles persistantes dans l'économie et dans la façon dont les rôles et les responsabilités sont désignés au foyer et dans la collectivité pour établir un régime officiel de domination/subordination qui leur permet de protéger et de prolonger leur privilège » (p.206).

[29] Woodlock 2016 : 587-588.
Le harcèlement facilité par les TIC peut donc être associé au phénomène que l'Internet et les médias ont surnommé la " vengeance-porn ", qui implique souvent l'humiliation publique de la victime.

[30] Voir https://www.wearethorn.org/sextortion/1880/ (lien vérifié pour la dernière fois le 12 septembre 2019).

2.1.2.3 Exploitation et abus sexuels d'enfants en ligne[31]

Les enfants semblent représenter un groupe primaire de victimes de la cyberviolence, en particulier en ce qui concerne la violence sexuelle en ligne.

Bien que « l'exploitation sexuelle et les abus sexuels d'enfants en ligne » ne soient pas nécessairement des formes nouvelles et distinctes d'exploitation et d'abus sexuels d'enfants, les TIC ont accru l'accessibilité des enfants pour les personnes qui cherchent à les exploiter et à les abuser sexuellement. Les TIC facilitent le partage d'images et de vidéos de l'abus sexuel et renforcent ainsi l'impact néfaste à long terme de l'abus des enfants. Les TIC contribuent également à faciliter l'exploitation sexuelle des enfants à des fins commerciales. Cependant, les TIC ne donnent pas lieu, en soi, à des types distincts d'infractions sexuelles contre les enfants.

L'exploitation et les abus sexuels d'enfants en ligne comprennent les comportements énumérés aux articles 18 à 23 de la Convention de Lanzarote[32] et à l'article 9 de la Convention de Budapest dans un environnement en ligne ou impliquant des systèmes informatiques :

- L'abus sexuel (article 18), c'est-à-dire « a) le fait de se livrer à des activités sexuelles avec un enfant qui, conformément aux dispositions pertinentes du droitnational, n'a pas atteint l'âge légal pour avoir des activités sexuelles ; ou b) le fait de se livrer à des activités sexuelles avec un enfant:
  - en faisant usage de la contrainte, de la force ou de menaces ; ou
  - en abusant d'une position reconnue de confiance, d'autorité ou d'influence sur l'enfant, y compris au sein de la famille ; ou
  - en abusant d'une situation particulièrement vulnérable de l'enfant, notamment en raison d'un handicap physique ou mental ou d'une situation de dépendance. »

- La prostitution enfantine (article 19), c'est-à-dire « a) le fait de recruter un enfant pour qu'il se livre à la prostitution ou de favoriser la participation d'unenfant à la prostitution ; b) le fait de contraindre un enfant à se livrer à la prostitution ou d'en tirer profit ou d'exploiter un enfant de toute autre manière à de telles fins ; ou c) le fait d'avoir recours à la prostitution d'enfant ».

- La pornographie mettant en scène des enfants (article 20), c'est-à-dire « a) la production de pornographie enfantine; b) l'offre ou la mise à disposition de pornographie enfantine ; c) la diffusion ou la transmission de pornographie enfantine ; d) le fait de se procurer ou de procurer à autrui de la pornographie enfantine; e) la possession de pornographie enfantine ; f) le fait d'accéder, en connaissance de cause et par le biais des technologies de communication et d'information, à de la pornographie enfantine ». On entend par « pornographie mettant en scène des enfants » tout matériel représentant visuellement un enfant se livrant à un comportement sexuellement explicite, réel ou simulé, ou toute représentation des organes sexuels d'un enfant à des fins essentiellement sexuelles.[33]

[31] Les réponses du Mexique suggèrent d'étendre ce concept aux « autres personnes dépendantes » telles que les personnes handicapées.
[32] Convention du Conseil de l'Europe pour la protection des enfants contre l'exploitation et les abus sexuels (STCE 201) http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/201
[33] Voir aussi l'article 9 de la Convention de Budapest.
Si le terme « pornographie mettant en scène des enfants » est utilisé dans les instruments internationaux (y compris les Conventions de Budapest et de Lanzarote) et dans le droit interne de nombreux pays, ce terme et ce concept ont également été contestés. Voir, par exemple, https://www.interpol.int/News-and-media/News/2018/N2018-010.
Ainsi, si l'on ne peut ignorer que le terme « pornographie mettant en scène des enfants » désigne une infraction spécifique et constitue la base de l'action de la justice pénale dans un grand nombre de pays, ce concept a ses limites et doit être utilisé avec prudence.

- La corruption d'enfants (article 22), c'est-à-dire « le fait intentionnel de faire assister, à des fins sexuelles, un enfant n'ayant pas atteint l'âge [au-dessous duquel il est interdit de se livrer à des activités sexuelles avec un enfant] d'être témoin d'abus sexuels ou d'activités sexuelles, même sans qu'il y participe, à des abus sexuels ou à des activités sexuelles. ».

- La « sollicitation d'enfants à des fins sexuelles » (article 23) - également appelée « grooming » - c'est-à-dire « le fait pour un adulte de proposer intentionnellement, par le biais des technologies de communication et d'information, une rencontre à un enfant n'ayant pas atteint l'âge fixé [au-dessous duquel il est interdit d'avoir des relations sexuelles avec un enfant] dans le but de commettre à son encontre une infraction établie conformément aux articles 18, paragraphe 1.a[se livrer à des activités sexuelles avec un enfant], ou 20, paragraphe 1.a[produire de la pornographie mettant en scène des enfants], lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre ».

L'exploitation sexuelle et les abus sexuels en ligne sont les principales formes de cyberviolence ciblant les enfants. Il convient toutefois de garder à l'esprit que les enfants sont également victimes d'autres types de cyberviolence. Une cartographie utile peut être tirée de l' « Étude sur les effets des nouvelles technologies de l'information sur la maltraitance et l'exploitation des enfants ».[34] S'appuyant sur des analyses antérieures, y compris le projet de l'UE pour un internet plus sûr, l'étude suggère les domaines suivants :

- « Matériel d'abus pédosexuels» ;
- « Exploitation sexuelle des enfants à des fins commerciales » ;
- « Cyber authentification, sollicitation et sollicitations sexuelles en ligne d'enfants » ;
- « la cyberintimidation, le harcèlement criminel et le harcèlement criminel»
- « Exposition à des contenus préjudiciables » .

2.1.2.4 Crimes haineux liés aux TIC

La cyberviolence peut être motivée par « un préjugé à l'encontre de la caractéristique personnelle perçue de la victime ou d'une appartenance perçue à un groupe de la victime. Ces groupes ou caractéristiques comprennent, sans toutefois s'y limiter, la race, l'origine ethnique, la religion, l'orientation sexuelle ou le handicap. » [35]

Elle inclut les comportements qui peuvent être criminalisés en vertu du Protocole additionnel à la Convention de Budapest sur la xénophobie et le racisme (STE 189).

Les crimes haineux ont de graves conséquences pour les individus et les sociétés et peuvent conduire à la violence communautaire et à la déstabilisation de sociétés entières.

Le Groupe a toutefois conclu qu'il ne serait pas possible de dresser un tableau complet de la question des crimes motivés par la haine dans le cadre du mandat et des délais fixés par le T-CY.

[34] (ONUDC 2015) https://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf
[35] https://www.uclan.ac.uk/research/explore/projects/assets/Hate_Crime_Survey_Report.pdfAu Royaume-Uni, par exemple, la police et le Crown Prosecution Service « se sont entendus sur la définition suivante pour identifier et signaler les crimes haineux : Toute infraction pénale qui est perçue par la victime ou toute autre personne comme étant motivée par l'hostilité ou un préjugé, fondé sur le handicap d'une personne ou la perception d'un handicap, la race ou la perception d'une race, la religion ou la perception d'une religion, l'orientation sexuelle ou la perception d'une orientation sexuelle, ou une personne transgenre ou perçue comme transsexuelle. »
https://www.cps.gov.uk/hate-crime

2.1.2.5 Menaces directes liées aux TIC ou violence réelle

La cyberviolence comprend également les menaces directes de violence ou la violence physique directe. Les systèmes informatiques peuvent être utilisés en cas de meurtre, d'enlèvement, de viol et d'autres actes de violence sexuelle ou d'extorsion.

Les formes de violence directe comprennent l'interférence avec des dispositifs médicaux causant des blessures ou la mort,[36] ou les attaques contre des infrastructures critiques au moyen d'ordinateurs. « Le swatting » ou canular téléphonique en est un autre exemple.

2.1.2.5.1 Le canular téléphonique

Le canular téléphonique ou « Swatting » est un exemple de la façon dont les systèmes informatiques peuvent être utilisés à mauvais escient pour de nombreux types de conduite ayant un impact violent sur les victimes. Il s'agit de l'utilisation de téléphones et souvent de systèmes informatiques pour tromper un service d'urgence afin d'envoyer les forces de l'ordre à un endroit précis sur la base d'une fausse déclaration. Le nom vient de l'acronyme « S.W.A.T. » (Armes et tactiques spéciales) qui sont des unités d'application de la loi ayant reçu une formation spécialisée et pouvant utiliser du matériel de type militaire. Ces faux rapports incluent le signalement d'homicides au domicile d'une tiers personne, les alertes à la bombe et les enlèvements. Le canular téléphonique peut tomber sous le coup de diverses lois criminelles, telles que les menaces de mort, le complot en vue de commettre une fraude, l'obstruction à la justice et les méfaits publics. Il ne s'agit pas de simples farces et attrapes téléphoniques : les auteurs de ces actes ont généralement recours à l'usurpation de l'identité de l'appelant et à l'ingénierie sociale, et certains utilisent des systèmes informatiques et des logiciels sophistiqués afin de faire croire que les appels proviennent d'endroits différents (parfois de pays différents du point de départ de l'auteur).[37] Le canular téléphonique peut être terrifiant et dangereux pour les victimes, qui ont été tuées par les forces de l'ordre ou qui ont subi des blessures physiques telles que des blessures par balle et des crises cardiaques.[38]

2.1.2.6 Cybercriminalité

Compte tenu de la définition proposée ci-dessus, certaines formes de cybercriminalité peuvent également être considérées comme des actes de cyberviolence, tels que l'accès illégal à des données personnelles intimes, la destruction de données, le blocage de l'accès à un système informatique ou de données, etc. C'est le cas, par exemple, du paragraphe 1030(a)(7) du United States Code Section 1030(a)(7) sur « l'extorsion de fonds par ordinateur ».

Les attaques par déni de service peuvent entraîner des dommages corporels aux personnes - par exemple, si les lignes téléphoniques d'urgence en cas d'incendie ne peuvent pas recevoir les appels ou si les systèmes de contrôle du trafic ou les services hospitaliers sont désactivés.

---

[36] https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

[37] En 2009, Matthew Weigman, un phreaker aveugle, a été condamné à 11 ans de prison aux États-Unis pour avoir écrasé des animaux. En 2014 en Colombie-Britannique, au Canada, un adolescent utilisant la poignée "Obnoxious" a commis 40 tentatives ou succès d'écrasement dans plusieurs pays. Il a plaidé coupable à 23 accusations.

[38] https://www.justice.gov/usao-md/pr/british-and-american-men-indicted-swatting ; https://www.fbi.gov/news/stories/the-crime-of-swatting-fake-9-1-1-calls-have-real-consequences1 ; https://www.fbi.gov/contact-us/field-offices/minneapolis/news/press-releases/houston-texas-area-teenager-sentenced-to-more-than-three-years-in-prison-for-swatting-and-making-bomb-threats-to-minnesota-high-school
Pour une affaire récente (décembre 2017) aux conséquences fatales, voir http://www.nydailynews.com/news/national/unarmed-kan-man-killed-cops-victim-swatting-prank-article-1.3726171
Selon ce rapport, le FBI estime qu'il y a environ 400 cas de frappe par an aux États-Unis.

2.2 Statistiques

Un nombre croissant d'études - dont beaucoup contiennent des données statistiques - sont disponibles sur différents aspects de la cyberviolence, en particulier sur les enfants, comme le montrent les exemples suivants.

Étant donné que les concepts et les définitions n'ont pas encore fait l'objet d'un accord et que la cyberviolence est souvent un continuum de violence hors ligne, il est difficile de comparer différents ensembles de données et d'arriver à une évaluation globale de l'ampleur et de l'impact de la cyberviolence.

On peut néanmoins conclure sans risque de se tromper que la cyberviolence est un problème croissant qui a un impact significatif sur un nombre croissant d'individus, en particulier les femmes et les enfants, dans de nombreuses régions du monde.

2.2.1 Données sur la cyberviolence contre les enfants

2.2.1.1 Cyberintimidation

Un projet de recherche mené entre juillet et octobre 2016 montre que, sur un échantillon national représentatif de 5 700 élèves âgés de 12 à 17 ans aux Etats-Unis, 33,8% des élèves ont été victimes de cyberintimidation,[39] par exemple par des commentaires méchants ou blessants en ligne (22.5 %), les rumeurs en ligne (20,1 %), l'affichage de commentaires méchants ou sexuels (12,7 %), les menaces en ligne (11,9 %), l'affichage de photos méchantes ou blessantes (11,1 %), l'usurpation d'identité (10,3 %) ou les commentaires désobligeants sur la race ou la couleur (10,1 %).

Bien que l'intimidation ne soit pas un phénomène nouveau, la disponibilité des médias sociaux, des applications et des appareils mobiles dotés de caméras intégrées favorise la propagation de la cyberintimidation.[40] Les hommes et les femmes en sont victimes, mais les délinquants sont plus souvent des hommes aux États-Unis.[41]

Une enquête publiée par Vodafone en septembre 2015[42] montre comment la cyberintimidation est perçue dans onze pays (République tchèque, Allemagne, Grèce, Irlande, Italie, Pays-Bas, Nouvelle-Zélande, Afrique du Sud, Espagne, Royaume-Uni et Etats-Unis). Les enfants de 13 à 18 ans ont été le plus souvent victimes d'intimidation en Nouvelle-Zélande (30 %), suivie des États-Unis (27 %) et de l'Irlande (26 %), tandis que les enfants de la République tchèque (8 %), de l'Espagne (8 %) et de l'Italie (11 %) ont été le moins souvent victimes d'intimidation.

La cyberintimidation est également un problème important dans les pays asiatiques. Par exemple, en Malaisie, un site Web[43] signale que :

- 33 % des enfants malaisiens ont été intimidés en ligne ;
- 15% ont commis des actes de cyberintimidation ;
- 27 % des parents malaisiens mettent leurs enfants en garde contre les risques liés à l'utilisation d'Internet, mais seulement 18 % éduquent leurs enfants sur les bons comportements à avoir en ligne.

[39] Voir http://cyberbullying.org/2015-data (lien vérifié le 13 septembre 2019).
[40] Pour des statistiques sur la cyberintimidation et les médias sociaux, voir http://www.meganmeierfoundation.org/cyberbullying-social-media.html (lien consulté le 3 avril 2017).
[41] Voir http://cyberbullying.org/2015-data (lien vérifié le 3 avril 2017).
[42] http://www.vodafone.com/content/index/media/vodafone-group-releases/2015/groudbreaking_global_survey.html
[43] Voir https://nobullying.com/bullying-in-malaysia-2/ (lien vérifié le 26 juillet 2017).

Une étude DiGi CyberSafe réalisée[44] en 2014 sur un échantillon de 14 000 écoliers en Malaisie l'a montré :

- environ 26 % des enfants malaisiens ont été victimes d'intimidation sur Internet, les jeunes de 13 à 15 ans étant les cibles les plus fréquentes ;
- le niveau de harcèlement en ligne est passé à 70 %, les insultes et l'affichage de messages ou de photos inappropriés sur les médias sociaux étant les infractions les plus courantes ;
- en même temps, 64% des jeunes n'ont pas considéré l'envoi de SMS inappropriés, l'affichage de photos inappropriées et le fait de se faire passer pour quelqu'un d'autre comme des actes d'intimidation en ligne ;
- 40 % des enfants interrogés ont déclaré qu'ils ne sauraient pas comment gérer l'intimidation ou se protéger en ligne ;
- les deux tiers des enfants de 13 ans et moins ont pris peu ou pas de mesures de protection lorsqu'ils naviguaient sur Internet ; pourtant, 53 % d'entre eux croyaient pouvoir naviguer sur Internet en toute sécurité ;
- environ 70 % des enfants de moins de 13 ans se sont montrés peu préoccupés par l'atteinte à leur vie privée ou par le fait de savoir avec qui ils interagissent en ligne ;
- plus de 40 % des jeunes qui considéraient que la sécurité en ligne était importante exerçaient de faibles niveaux de protection en ligne.

Une enquête réalisée [45] par Stairway Foundation Inc. a montré qu'aux Philippines, sur un échantillon de 1 268 enfants âgés de 7 à 12 ans et 1 143 enfants âgés de 13 à 16 ans :

- 80 % des adolescents de 13 à 16 ans sont victimes de cyberintimidation par le biais des médias sociaux, tandis que 60 % de leurs homologues âgés de 7 à 12 ans ont subi les mêmes abus ;
- 30 % des enfants de 7 à 12 ans ont été intimidés par des menaces et 10 % ont été humiliés ou ont vu leurs conversations privées exposées ;
- 30 % des adolescents de 13 à 16 ans ont été victimes d'intimidation par le biais de la retouche photo ;
- L'enquête montre également que, pour les deux groupes, 20 % des cyberintimidateurs sont des personnes qui utilisent de faux profils en ligne.

Ces études et d'autres indiquent que les enfants sont touchés de façon disproportionnée par la cyberviolence sous la forme de cyberintimidation.

2.2.1.2 Violence sexuelle en ligne contre les enfants

De nombreux rapports soulignent l'ampleur de la violence sexuelle contre les enfants sur Internet.

Par exemple, en 2016, selon le Rapport annuel 2016 de l'Internet Watch Foundation du Royaume-Uni[46] - basé sur des rapports reçus de 16 portails dans le monde :

- le nombre de domaines hébergeant des images d'abus pédosexuels est passé de 1 991 en 2015 à 2 415 en 2016, soit une augmentation de 21 % ;
- 57 335 des 102 932 adresses URL signalées contenaient des images d'abus pédosexuels ;
- 455 groupes de discussion ont été confirmés comme contenant des images d'abus pédosexuels ;

[44] http://www.digi.com.my/aboutus/media/press_release_detail.do?id=8600age=1ear=2014
[45] Voir "*Cybersafe survey 2015*" http://www.cybersafe.asia/wp-content/uploads/2016/03/Cybersafe-Survey_LOWRES.pdf (consulté le 13 septembre 2019).
[46] https://www.iwf.org.uk/sites/default/files/reports/2017-04/iwf_report_2016.pdf

- 53 % des enfants représentés dans les images ont été évalués comme étant âgés de 10 ans ou moins.

L'ampleur de la violence sexuelle à l'égard des enfants en ligne se reflète également dans les opérations de maintien de l'ordre. Par exemple, le démantèlement de Playpen - l'un des plus grands sites d'abus pédosexuels au monde avec plus de 150 000 utilisateurs dans le monde - et l'opération « Pacifier » qui a suivi, ont conduit à l'arrestation de 368 pédophiles présumés en Europe, alors que l'administrateur principal de Playpen a été condamné à 30 ans de prison aux Etats-Unis en mai 2017.[47]

INTERPOL a signalé que 10 000 victimes d'abus pédosexuels ont été identifiées grâce à sa base de données internationale sur l'exploitation sexuelle des enfants (ICSE).[48]
Il ne fait donc aucun doute que les enfants sont touchés de manière disproportionnée par la violence sexuelle en ligne.

2.2.2 Données sur la cyberviolence contre les femmes

Si la question de la cyberintimidation impliquant des enfants fait l'objet de recherches approfondies, les études statistiques portant sur la cyberviolence contre les femmes dans différentes régions du monde peuvent être moins répandues.

Le rapport 2015 du49 Département des affaires économiques et sociales des Nations Unies, « The World's Women 2015, Trends and Statistics », a montré que « 1 femme sur 3 a subi des violences physiques/sexuelles à un moment donné de sa vie », mais les données sur le rôle des TIC - à l'exception d'une brève référence aux téléphones mobiles et aux médias sociaux - manquent.

En 2014, l'Agence des droits fondamentaux de l'UE (FRA) a publié une enquête détaillée sur « La violence à l'égard des femmes : une enquête européenne ».[50] Selon cette enquête, au cours des douze mois précédant l'enquête :

- environ 7 % des femmes âgées de 18 à 74 ans (soit 13 millions de femmes dans les 28 États membres de l'UE) ont subi des violences physiques ;
- environ 2 % (3,7 millions) ont été victimes de violences sexuelles ;
- environ 5% (9 millions) ont connu des situations « où la même personne a été à plusieurs reprises offensante ou menaçante » à leur égard à l'égard d'une liste d'actions différentes ; par exemple, la même personne a à plusieurs reprises « traîné ou attendu en dehors de votre domicile, lieu de travail ou école sans raison légitime ; » ou « vous a appelé de façon offensante, menaçante ou silencieuse au téléphone » ;
- environ 5% (9 millions) - dont 11% dans le groupe d'âge des 18 à 29 ans - avaient été victimes de « formes de cyberharcèlement sexuel... y compris des courriels sexuellement explicites non désirés ou des messages SMS offensants ». Quelque 11 % (plus de 20 millions) avaient été victimes de cyberharcèlement depuis l'âge de 15 ans ;
- environ 5 % (9 millions) avaient fait l'objet de harcèlement criminel, et 23 % d'entre eux « ont dû changer leur adresse électronique ou leur numéro de téléphone en réponse au cas le plus grave de harcèlement criminel. »

[51]Un rapport publié en 2017 par le Pew Research Center sur le harcèlement en ligne aux États-Unis a révélé que, sur un échantillon de 4 248 adultes :

[47] https://www.europol.europa.eu/newsroom/news/major-online-child-sexual-abuse-operation-leads-to-368-arrests-in-europe
[48] http://virtualglobaltaskforce.com/2017/interpol-network-identifies-10000-child-sexual-abuse-victims/
[49] https://unstats.un.org/unsd/gender/chapter6/chapter6.html
[50] http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

- 41 % des Américains ont été personnellement victimes de harcèlement en ligne, et une proportion encore plus grande (66 %) ont été témoins d'un tel comportement envers autrui ;
- près de 18 % ont fait l'objet de formes particulièrement graves de harcèlement en ligne, telles que les menaces physiques, le harcèlement sur une période prolongée, le harcèlement sexuel ou le harcèlement criminel ;
- Les plateformes de médias sociaux sont un terrain particulièrement fertile pour le harcèlement en ligne qui cible habituellement une caractéristique personnelle ou physique, c'est-à-dire que 14 % des Américains disent avoir été harcelés en ligne spécifiquement en raison de leurs opinions politiques, alors qu'environ 9 % ont été ciblés en raison de leur apparence physique et 8 % pour leur race, ethnicité ou sexe ;
- Dans l'ensemble, les hommes sont un peu plus susceptibles d'être victimes d'une certaine forme de harcèlement en ligne, mais les femmes - et surtout les jeunes femmes - font face à des taux plus élevés de formes de violence sexuelle. Environ 21 % des femmes de 18 à 29 ans déclarent avoir été victimes de harcèlement sexuel en ligne. De plus, environ la moitié (53 %) des jeunes femmes de 18 à 29 ans déclarent que quelqu'un leur a déjà envoyé des images explicites qu'elles n'avaient pas demandées.[52]

Un rapport de 2016 sur la cyberviolence à l'égard des femmes et des minorités en Inde[53] l'affirme :

- Parmi les 500 personnes interrogées (dont 97 % étaient des femmes), 58 % ont déclaré avoir été victimes d'une forme quelconque d'agression en ligne sous forme de harcèlement, d'intimidation, d'abus ou de harcèlement ;
- 36 % des répondants qui avaient été victimes de harcèlement en ligne n'ont rien fait du tout. 38 % ont déclaré qu'ils avaient intentionnellement réduit leur présence en ligne après avoir subi des abus en ligne ;
- Les femmes ont trouvé difficile de considérer le harcèlement en ligne comme étant comparable à la violence, même si 30 % de celles qui l'ont vécu l'ont trouvé « extrêmement perturbant » et 15 % ont rapporté qu'il mène à des problèmes de santé mentale comme la dépression, le stress et l'insomnie ;
- seulement un tiers des répondants avaient signalé le harcèlement aux organismes d'application de la loi ; parmi eux, 38 % ont qualifié la réponse de " pas utile du tout ".

Un rapport sur « Women's Rights Online » de 2015[54] - couvrant neuf villes d'Afrique et d'Asie - a identifié le harcèlement en ligne comme l'une des contraintes limitant l'utilisation de la technologie par les femmes. Selon l'étude :

- « Dans l'ensemble, le nombre de cas de harcèlement et d'abus signalés était faible. Seulement 13 % environ des femmes (et 18 % des hommes) ont déclaré avoir été victimes de tels incidents par téléphone ou par SMS, tandis que 13 % des femmes et 11 % des hommes qui utilisent l'Internet ont été victimes d'abus par courrier électronique ou par les médias sociaux » ;
- Cependant, dans certaines villes, un grand nombre de femmes, mais aussi d'hommes, ont été victimes d' »intimidation personnelle (y compris de harcèlement ou de harcèlement) » au cours des deux dernières années lorsqu'ils utilisaient un téléphone portable (par exemple, 28% des femmes à Jakarta, 21% des femmes à Kampala, 60%

[51] Voir Pew Research Center, juillet 2017, "*Online Harassment 2017*" http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/07/10151519/PI_2017.07.11_Online-Harassment_FINAL.pdf (site consulté le 13 septembre 2019).
[52] Voir Pew Research Center, juillet 2017, "*Online Harassment 2017*", p. 7.
[53] Voir le rapport *"'Violence' Online in India : Cybercrimes Against Women & Minorities on Social Media"* https://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf
[54] http://webfoundation.org/docs/2015/10/womens-rights-online21102015.pdf

des hommes à Nairobi) ou Internet (45% des femmes à Kampala, 21% des femmes et 19% des hommes à Nairobi).

Selon une enquête sur l'aide aux femmes réalisée en 2017 :

- 45 % des victimes de violence familiale ont déclaré avoir été victimes de violence en ligne sous une forme ou une autre au cours de leur relation ;
- 48 % ont déclaré avoir été victimes de harcèlement ou d'abus en ligne de la part de leur ex-partenaire après avoir quitté leur relation. 38 % ont déclaré avoir été harcelés en ligne après avoir quitté leur relation ;
- 75 % ont dit craindre que la police ne sache pas comment réagir au mieux aux abus ou au harcèlement en ligne. Cela comprend 12 % de ceux qui avaient signalé les mauvais traitements à la police et qui n'avaient pas reçu d'aide55.

2.3 Défis en matière d'enquêtes et de poursuites de le cyberviolence

La cyberviolence soulève toute une série de questions qui doivent être prises en considération. Par exemple :

- Les victimes n'ont aucune information sur les recours disponibles :
  Un aspect particulièrement désolant de la cyberviolence est que les victimes peuvent ne pas savoir comment obtenir de l'aide. Il se peut qu'on les avertisse violemment de ne pas contacter les forces de l'ordre et qu'ils ne sachent pas à qui s'adresser de toute façon (voir la discussion ci-dessous). Leurs méthodes normales de communication peuvent être coupées ou compromises et une attaque soutenue peut les choquer et les perturber à un point tel que leur capacité à se défendre ou même à penser correctement peut être diminuée.[56]

- Aide limitée de la part des forces de l'ordre :
  Les victimes peuvent avoir l'impression que l'application de la loi n'a pas été d'une grande utilité, ou qu'il a fallu beaucoup de persévérance pour obtenir une aide utile. La cyberviolence peut impliquer des méthodes qui sont particulièrement difficiles à mettre en œuvre pour les forces de police, et les victimes peuvent se faire dire - à tort ou à raison - qu'il n'y a rien que la police puisse faire. Comme toute autre forme de violence à l'égard des femmes, la violence en ligne à l'égard des femmes est souvent négligée en raison d'un manque de sensibilisation et de compréhension de la violence sexiste. L'expérience des victimes est souvent considérée comme un « incident » plutôt que comme un modèle de comportement, et les victimes sont blâmées pour la violence qu'elles subissent. Ainsi, la plainte d'une seule personne peut ne pas révéler qu'elle fait partie d'une tendance plus large selon laquelle un auteur particulier peut cibler des douzaines de victimes dans plusieurs juridictions, comme ce fut le cas avec Aydin Coban qui a victimisé plus d'une trentaine de filles et garçons adolescents dans plusieurs pays dont les Pays-Bas et le Canada (entraînant le suicide de la jeune Amanda Todd,

[55] Clare Laxton, Women's Aid, Virtual World, Real Fear, Women's Aid report into online abuse, harassment and stalking, 2014, disponible en ligne à http://bit.ly/2h0W4OX.
[56] NATIONAL CENTER FOR VICTIMS OF CRIME, "Are You Being Stalked ?", http://victimsofcrime.org/docs/src/aybs_english_color.pdf?sfvrsn=4 ; CANADIAN DEPARTMENT OF JUSTICE, "A Handbook for Police and Crown Prosecutors on Criminal Harassment", 2017-01-09, http://www.justice.gc.ca/eng/rp-pr/cj-jp/fv-vf/har/part1.html https://www.justice.gov/usao-ak/pr/anchorage-man-sentenced-cyberstalking-former-girlfriend ; https://www.justice.gov/usao-wdny/pr/former-irondequoit-police-officer-sentenced-cyber-stalking-his-ex-girlfriend ; https://www.justice.gov/opa/pr/new-hampshire-man-sentenced-prison-computer-hacking-and-sextortion-scheme-involving-multiple https://www.justice.gov/opa/pr/former-us-state-department-employee-pleads-guilty-extensive-computer-hacking-cyberstalking

15 ans)[57]. Dans certains pays, seules certaines forces de police sont habilitées à enquêter sur de tels crimes. Il peut être difficile pour les victimes de savoir vers quelle unité se tourner ou, en pratique, il peut être difficile de travailler avec l'unité (si l'unité est dans la capitale et que la victime est à des centaines de kilomètres de distance). Les victimes peuvent aussi rencontrer des agents de la force publique ou des fonctionnaires qui ne sont pas au courant du phénomène et ne comprennent pas la gravité potentielle du phénomène. Enfin, il se peut que le droit local ne traite pas de certains types d'attaques en droit pénal (peut-être pour des raisons valables), de sorte qu'il n'y a tout simplement pas de base juridique pour engager des poursuites.[58]

- Protection des enfants contre protection des victimes adultes :
  Les enfants peuvent, dans une certaine mesure, être mieux protégés que les adultes parce que les lois sur l'exploitation des enfants peuvent être utilisées pour couvrir la cyberviolence contre les enfants. Si une jeune fille de 14 ans est traquée et filmée en secret, par exemple, les lois sur l'exploitation des enfants peuvent faire l'objet de poursuites. Toutefois, les lois d'un pays peuvent ne pas offrir la même protection à une femme de 19 ans.[59]

- Rôle des fournisseurs de médias sociaux :
  Diverses plates-formes Internet/médias sociaux peuvent jouer un rôle dans la cyberviolence. L'information sur les médias sociaux peut être utilisée pour identifier et localiser les victimes, pour connaître leurs vulnérabilités (quelles journées de travail et leurs heures de déplacement, par exemple), pour recueillir des détails à leur sujet et pour d'autres fins. D'autres plates-formes peuvent être utilisées pour afficher des

[57] http://www.cbc.ca/news/canada/british-columbia/aydin-coban-sentenced-netherlands-online-fraud-blackmail-1.4027359

[58] HM CROWN PROSECUTION SERVICE INSPECTORATE AND HM INSPECTORATE OF CONSTABULARY, " Living in fear - the police and CPS response to harassment and stalking - A joint inspection by HMIC and HMCPSI, " juillet 2017, http://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/living-in-fear-the-police-and-cps-response-to-harassment-and-stalking.pdf ; CAUTERUCCI, CHRISTINA, CHRISTINA, slate.com, "English Police Apologize to a Woman Who Reported Her Stalker 125 times Before He Stabbed Her", 29 juin 2017, http://www.slate.com/blogs/xx_factor/2017/06/29/english_police_apologize_to_helen_pearson_who_reported_her_stalker_125_times.html ; KHAN, SOHAIL, Hindustan Times, "Cop'victim-shames' minor facing harassment on social media, Maneka intervenes", 12 avril 2017, http://www.hindustantimes.com/india-news/cop-victim-shames-minor-facing-harassment-on-social-media-maneka-intervenes/story-jF3bFnX1SL10f3UJci7ApJ.BAUM, KATRINA, et al, Bureau of Justice Statistics, U.S. Department of Justice Office of Justice Programs, " National Crime Victimization Survey Stalking Victimizationization in the United States ", 2009, https://victimsofcrime.org/docs/src/baum-k-catalano-s-rand-m-rose-k-2009.pdf?sfvrsn=0 ; CANADIAN RESOURCE CENTRE FOR VICTIMS OF CRIME, cyberstalking information paper, https://crcvc.ca/docs/cyberstalking.pdf ; FEMINISM IN INDIA.COM, *" Violence" Online In India : Cybercrimes contre les femmes et les minorités sur les médias sociaux"* https://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf ; SYNDICAT INTERPARLEMENTAIRE, "Sexisme, harcèlement et violence contre les femmes parlementaires", octobre 2016, https://ipu.org/resources/publications/reports/2016-10/sexism-harassment-and-violence-against-women-parliamentarians ; INITIATIVE CYBER CIVIL RIGHTS, FAQs, "On me dit que je devrais déposer un rapport de police, que devrais-je savoir avant de le faire ? "Les victimes ne sont-elles pas protégées par les lois criminelles existantes contre le harcèlement criminel, le harcèlement criminel et le voyeurisme "The University of Maryland Francis King Carey School of Law and United States Department of Justice (DOJ) Cybercrime Symposium,*When Cybercrime Turns Violent and Abusive",* 15 septembre 2017, discussion en groupe : "Holding Offenders Accountable ", http://www.law.umaryland.edu/about/news_details.html?news=2218 ; CHIARINI, Annmarie, discours liminaire au symposium, https://www.youtube.com/watch?v=G6cdN3TzDlondex=4ist=PLYBWqedwTFEZq8RB1mOVc20zOmIhMd-Fi (liens vérifiés le 13 septembre 2019).
https://www.buzzfeed.com/mariekirschen/que-faire-quand-vous-etes-victime-ou-temoin-de-cyberharcelem?utm_term=.cu9dBjy06#.wak7N8ZRy
https://www.francetvinfo.fr/economie/emploi/metiers/droit-et-justice/on-se-retrouve-seule-avec-cette-violence-les-victimes-de-cyberharcelement-demunies-face-a-la-difficile-traque-des-auteurs_2459358.html
https://www.ccmm.asso.fr/chroniques-de-limpunite-2-0-docu-edifiant-cyber-harcelement/
http://www.sueddeutsche.de/leben/stalking-die-saat-der-angst-1.2722886-3
https://www.welt.de/vermischtes/article132273264/Ich-dachte-ich-drehe-durch.html

[59] Il peut y avoir des raisons valables de différencier en droit pénal entre le niveau de protection accordé aux enfants et la protection accordée aux adultes.

messages de victimisation - par exemple des sollicitations pour viol - ou pour menacer des cibles.

Bien entendu, certaines plateformes ont pour modèle d'affaires de favoriser la criminalité, de sorte que les plaintes et les renvois ne sont pas pertinents pour elles. D'autres plateformes offrent des mécanismes de plaintes ou de suppression d'affichages. Ces mécanismes peuvent ne pas être suffisants ou assez rapides, et les victimes peuvent trouver qu'une affectation a été largement diffusée et qu'il est inutile de l'envoyer à un seul endroit.

Dans certains pays, des groupes ont commencé à protester contre l'inaction des prestataires. Les plates-formes Internet, en particulier celles qui disposent d'une large portée et d'un personnel suffisant, ont la possibilité de prendre des mesures actives contre la cyberviolence, notamment en supprimant des messages et en préservant les preuves.[60]

En janvier 2018, Facebook aurait conclu un accord en Irlande du Nord avec une adolescente victime de pornographie de vengeance « après que sa photo[intime] soit apparue plusieurs fois entre novembre 2014 et janvier 2016. Elle a allégué une mauvaise utilisation des renseignements personnels, de la négligence et une violation de la Loi sur la protection des données. Ses avocats (....) ont affirmé que le règlement avait « déplacé les poteaux de but » quant à la façon dont les réseaux de médias sociaux tels que Facebook devraient réagir aux messages et images indécents et abusifs affichés sur leurs sites ».[61]

- Liberté d'expression contre discours haineux :

  Les pays ont des points de vue différents sur la mesure dans laquelle la parole devrait être limitée par la société - c'est-à-dire où établir l'équilibre entre le droit fondamental d'une personne à s'exprimer et le droit fondamental d'une autre personne à la sécurité. Par exemple, un site Web peut afficher les écoles fréquentées par les enfants de la police, avec des photos des enfants. Si aucune menace explicite n'est incluse sur le site, les pays peuvent différer quant à savoir si de tels messages constituent des propos illégaux. Si une menace explicite est incluse, les pays peuvent toujours différer sur le point de savoir si elle est suffisamment grave pour constituer un crime.

  De nombreux pays restreignent ou interdisent le discours haineux, normalement défini comme une expression qui s'attaque à des groupes identifiables distincts, tels que les groupes religieux, ethniques ou nationaux.

  Les États-Unis ne limitent pas les discours de haine en l'absence d'un niveau de danger suffisant. Compte tenu de la concentration actuelle des données soumises au droit américain, le droit interne américain a une grande influence sur l'Internet. Son rejet de nombreuses restrictions à la liberté d'expression a des répercussions sur les personnes qui se trouvent à l'extérieur des États-Unis. De plus, en raison de la loi américaine, le gouvernement américain refuse parfois de fournir une assistance juridique mutuelle dans les affaires impliquant des propos haineux.

  En tant qu'entités privées, les fournisseurs sont autorisés par la loi américaine à établir leurs propres règles concernant le matériel qu'ils transportent sur leurs systèmes. Certains choisissent de réglementer le contenu, mais d'autres offrent une liberté de parole pouvant être illégale en dehors des États-Unis. Ces dernières années, les pays européens ont cherché à conclure des accords de coopération avec ces fournisseurs pour supprimer les propos illégaux au regard des normes européennes. Certains pays ont pris des mesures contraignantes pour faire exécuter ce renvoi.

[60] Voir https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[61] https://www.theguardian.com/technology/2018/jan/12/facebook-faces-legal-action-from-victims-of-revenge-porn

2.4 Cyberviolence à l'égard des femmes et des enfants telle qu'abordée par les Conventions d'Istanbul et de Lanzarote

Les Conventions de Budapest, de Lanzarote et d'Istanbul exigent l'incrimination de comportements spécifiques qui incluent ou impliquent la violence contre les femmes et les enfants.

2.4.1 "Convention de Lanzarote sur la protection des enfants contre l'exploitation et les abus sexuels (STCE 201)[62]

La Convention de Lanzarote dans son ensemble vise - par une approche holistique - la protection des enfants contre la violence sexuelle. Il couvre :

- des mesures préventives telles que le recrutement, la formation et la sensibilisation des personnes travaillant en contact avec les enfants (article 5), l'éducation des enfants (article 6), les programmes et mesures d'intervention préventive (article 7), les mesures pour le grand public (article 8) et la participation des enfants, le secteur privé, les médias et la société civile (article 9) ;

- les mesures de protection et d'assistance aux victimes, y compris le signalement des soupçons d'exploitation ou d'abus sexuels (article 12), les lignes d'assistance téléphonique (article 13), l'assistance aux victimes (article 14) ;

- programmes ou mesures d'intervention ;

- le droit pénal matériel, y compris
  - l'abus sexuel (article 18),
  - la prostitution des enfants (article 19),
  - pornographie enfantine (article 20),
  - la participation d'un enfant à des spectacles pornographiques (article 21),
  - corruption d'enfants (article 22),
  - la sollicitation d'enfants à des fins sexuelles (article 23) ;

- le droit des enquêtes, des poursuites et de la procédure, y compris les mesures visant à protéger et à respecter les droits, les intérêts et les besoins particuliers des enfants au cours des enquêtes et des procédures pénales ;

- la coopération internationale.

La Convention établit un mécanisme de suivi mis en place depuis 2011 sous la forme du « Comité de Lanzarote ».[63]

Les Parties à la Convention de Lanzarote ayant rencontré des difficultés en ce qui concerne l'application effective de l'article 23 (« sollicitations sexuelles »), le Comité de Lanzarote a adopté, le 17 juin 2015, un avis[64] sur la sollicitation des enfants à des fins sexuelles au moyen des technologies de l'information et des communications.

L'avis précise les obligations imposées aux parties par l'article 23, notamment l'incrimination de la proposition intentionnelle d'un adulte de rencontrer un enfant dans le but de commettre des actes sexuels illégaux à son égard. Cette proposition intentionnelle est organisée et exprimée au moyen

[62] http://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/0900001680084822
[63] https://www.coe.int/fr/web/children/lanzarote-committee
[64] Voir https://rm.coe.int/168064de98 (lien vérifié le 19 mai 2017).

des technologies de l'information et de la communication et doit être suivie d'actes matériels conduisant à une telle réunion.

L'avis réitère que les enfants peuvent être exposés à certains des mêmes risques en ligne que hors ligne, comme être persuadés de se livrer à un comportement sexuellement explicite réel ou simulé, être recrutés ou contraints de participer à des spectacles pornographiques, ou être témoins d'abus sexuels ou d'activités sexuelles, et que ces types de comportements illicites qui peuvent survenir en ligne sont criminalisés par d'autres dispositions de la Convention.[65]

L'avis donne des indications aux États qui souhaitent aller au-delà des exigences et du champ d'application de l'article 23, notamment en leur proposant d'ériger en infraction pénale la sollicitation, même dans les cas où celle-ci n'aboutit pas à une rencontre en personne mais reste exclusivement en ligne. L'avis note également que la responsabilité des enquêtes et des poursuites en matière de manipulation en ligne devrait continuer d'incomber aux autorités chargées de l'application de la loi et au système de justice pénale. Le cas échéant, une assistance peut être demandée à des ONG spécialisées, mais ni celles-ci ni le public ne devraient devenir de facto des services répressifs.

En outre, à la suite de l'adoption de l'avis susmentionné, le comité de Lanzarote a créé un groupe de travail chargé d'examiner les liens entre les abus sexuels et l'exploitation sexuelle et les nouvelles technologies (telles que le sexting, la « sextortion », la diffusion en direct des abus sexuels et autres phénomènes), et si ces phénomènes étaient suffisamment couverts par la convention de Lanzarote.

Sur la base des résultats de ce groupe de travail, le Comité de Lanzarote a approuvé lors de sa 18ème session plénière (10-12 mai 2017) l' « Avis interprétatif sur l'applicabilité de la Convention de Lanzarote aux infractions sexuelles contre les enfants facilitées par le recours aux technologies de l'information et de la communication (TIC) ».[66] En conséquence :

- Le Comité de Lanzarote s'accorde à penser que la Convention de Lanzarote établit que les Parties doivent protéger les enfants contre toutes les formes d'exploitation et d'abus sexuels, y compris celles facilitées par l'utilisation des TIC, même lorsque le texte de la Convention de Lanzarote ne mentionne pas expressément les TIC. Les infractions existantes dans la Convention de Lanzarote restent donc criminalisées par le droit national de la même manière, qu'elles aient été commises ou non au moyen des TIC.

- Le Comité de Lanzarote suggère que, « dans la mise en œuvre de la Convention de Lanzarote, les Parties devraient assurer une réponse appropriée au développement technologique et utiliser tous les outils, mesures et stratégies pertinents pour prévenir et combattre efficacement les infractions sexuelles contre les enfants, qui sont facilitées par le recours aux TIC ».

- Parmi les activités possibles à entreprendre, le Comité Lanzarote suggère que les Parties allouent des ressources pour assurer l'efficacité des enquêtes et des poursuites concernant les infractions sexuelles contre des enfants facilitées par l'utilisation des TIC et qu'une formation soit fournie aux autorités chargées des enquêtes et des poursuites. En outre, les parties encouragent la coopération entre les autorités publiques compétentes, la société civile et le secteur privé afin de mieux prévenir et combattre les abus et l'exploitation sexuels des enfants facilités par l'utilisation des TIC.

[65] A savoir les articles 20§1, 21§1, 22 et 24§2 de la Convention.
[66] https://rm.coe.int/t-es-2017-03-en-final-interpretative-opinion/168071cb4f (lien vérifié le 13 septembre 2019)

Le Comité de Lanzarote a ensuite lancé le 20 juin 2017 le 2e cycle de suivi de la Convention de Lanzarote en diffusant un questionnaire thématique sur la « Protection des enfants contre l'exploitation et les abus sexuels facilitée par les technologies de l'information et des communications (TIC) ». Le questionnaire concerne principalement la protection des enfants contre l'exploitation criminelle d'images et/ou de vidéos sexuellement explicites et d'autres contenus sexuels autogénérés. Les réponses des 42 Parties à la Convention de Lanzarote ont été publiées.[67] Ils seront examinés par le Comité de Lanzarote dans le courant des années 2018 et 2019 avec des commentaires sur les réponses soumises par la société civile et des contributions des enfants eux-mêmes.

Ainsi, comme indiqué ci-dessus, les dispositions de la Convention de Lanzarote s'appliquent à la violence sexuelle dans un environnement en ligne.

Un document de travail détaillé, préparé par le Projet mondial sur la cybercriminalité du Conseil de l'Europe en 2012, a montré comment les dispositions de droit pénal matériel des Conventions de Budapest et de Lanzarote peuvent servir de référence pour la législation nationale.[68]

En ce qui concerne le droit pénal matériel, les Conventions de Budapest et de Lanzarote ont une portée différente mais semblent complémentaires. Un pays appliquant la Convention de Budapest ne devrait donc pas se limiter à l'article 9 de la Convention de Budapest sur la pornographie mettant en scène des enfants, mais envisager également d'introduire les articles 18 à 23 de la Convention de Lanzarote dans son droit interne afin de couvrir la violence sexuelle contre les enfants.

La Convention de Lanzarote ne contient pas de dispositions spécifiques pour sécuriser les preuves électroniques dans les enquêtes nationales et internationales relatives à la violence sexuelle contre les enfants sur Internet. Les pays appliquant la Convention de Lanzarote devraient donc envisager d'introduire dans leur droit interne les pouvoirs procéduraux prévus aux articles 16 à 21 de la Convention de Budapest et de devenir parties à la Convention de Budapest pour faciliter la coopération internationale en matière de preuve électronique (articles 23 à 35 de la Convention de Budapest) en relation avec la violence sexuelle en ligne contre les enfants.[69]

2.4.2 Convention d'Istanbul sur la violence contre les femmes et la violence domestique (STCE 210)[70]

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, STCE 210) définit la « violence contre les femmes » à l'article 3 :

> comme une violation des droits de l'homme et une forme de discrimination à l'égard des femmes et désigne tous les actes de violence sexiste qui causent ou sont susceptibles de causer aux femmes un préjudice ou des souffrances physiques, sexuelles, psychologiques ou économiques, y compris la menace de tels actes, la contrainte ou la privation arbitraire de liberté, que ce soit en public ou dans la vie privée.

[67] Le questionnaire et les réponses reçues sont disponibles à l'adresse suivante https://www.coe.int/en/web/children/2nd-monitoring-round
[68] https://rm.coe.int/16802fa3e2
[69] Comme indiqué ailleurs, s'il est optimal pour les pays d'être Parties aux conventions de Lanzarote, d'Istanbul et de Budapest, les non-Parties peuvent bien entendu s'inspirer de ces conventions pour adopter leur législation nationale.
[70] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/210
Le GREVIO est l'organe d'experts indépendants chargé du suivi de la mise en œuvre de la Convention d'Istanbul. http://www.coe.int/en/web/istanbul-convention/grevio

Les comportements visés par plusieurs dispositions de droit pénal matériel peuvent se produire, au moins partiellement, dans un environnement en ligne. Ces dispositions sont donc pertinentes pour la présente étude cartographique :

> Article 33 - Violence psychologique
> Les Parties prennent les mesures législatives ou autres nécessaires pour ériger en infraction pénale le comportement intentionnel consistant à porter gravement atteinte à l'intégrité psychologique d'une personne par la contrainte ou la menace.
>
> Article 34 - Harcèlement
> Les Parties prennent les mesures législatives ou autres nécessaires pour ériger en infraction pénale le comportement intentionnel consistant à menacer de manière répétée une autre personne et à lui faire craindre pour sa sécurité.
>
> Article 40 - Harcèlement sexuel
> Les Parties prennent les mesures législatives ou autres nécessaires pour faire en sorte que toute forme de comportement non désiré, verbal, non verbal ou physique, de nature sexuelle, ayant pour but ou pour effet de porter atteinte à la dignité d'une personne, en particulier en créant un environnement intimidant, hostile, dégradant, humiliant ou offensant, fasse l'objet de sanctions pénales ou autres.

Aucun de ces articles ne mentionne explicitement les TIC, mais le Rapport explicatif, en ce qui concerne l'article 34, prend en considération le fait que le comportement menaçant peut consister à suivre la victime de manière répétée dans le monde virtuel (salons de discussion, sites de réseautage social, messagerie instantanée, etc.) S'engager dans une communication non désirée implique la poursuite de tout contact actif avec la victime par tous les moyens de communication disponibles, y compris les outils de communication modernes et les TIC.

Le GREVIO est l'organe d'experts indépendants chargé de suivre la mise en œuvre de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence faite aux femmes et la violence domestique[71]. Le GREVIO souligne « l'importance de considérer la cyberviolence et les formes de violence hors ligne contre les femmes et les filles comme une expression du même phénomène, à savoir la violence sexiste. La violence en ligne contre les femmes et les filles doit donc être considérée comme un continuum de violence hors ligne et comme un moyen de maintenir les femmes dans une position inférieure dans la sphère numérique et dans la vie réelle. »[72]

Au chapitre III (Prévention), l'article 17 de la Convention d'Istanbul fait spécifiquement référence à la participation du « secteur des technologies de l'information et de la communication » :

> Article 17 - Participation du secteur privé et des médias
>
> 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 des contenus dégradants à caractère sexuel ou violent qui peuvent être nuisibles.

[71] https://www.coe.int/en/web/istanbul-convention/grevio
[72] Le GREVIO commente un projet antérieur de la présente étude cartographique.

En 2016, le Conseil de l'Europe a publié une publication sur l'article 17[73] qui identifie quatre actions possibles que les gouvernements, le secteur privé et les médias peuvent prendre ensemble pour promouvoir des mesures visant à prévenir la violence contre les femmes et la violence domestique :

- améliorer la formation des professionnels des médias sur les questions liées à l'égalité des sexes et à la violence contre les femmes ;
- promouvoir l'autorégulation des médias et la réglementation des contenus discriminatoires et violents ;
- créer des partenariats pour accroître la couverture médiatique de l'égalité des sexes et de la violence contre les femmes ;
- promouvoir la coopération en matière d'éducation aux médias.

L'article 17 concerne la prévention et ces actions - et il en va de même pour la « liste de contrôle » détaillée à la fin de la publication - se veulent donc préventives et ne traitent pas de questions de justice pénale.

La Stratégie du Conseil de l'Europe en matière d'égalité entre les femmes et les hommes (2018-2023) comprend comme première stratégie la prévention et la lutte contre les stéréotypes et le sexisme, y compris ceux qui apparaissent en ligne.[74]

Ce qui a été observé en ce qui concerne la complémentarité des Conventions de Budapest et de Lanzarote peut s'appliquer modus modendi à la Convention d'Istanbul :

- En ce qui concerne le droit pénal matériel, les Conventions de Budapest et d'Istanbul semblent complémentaires. Un pays qui applique la Convention de Budapest devrait donc envisager d'appliquer également les articles 33, 34 et 40 de la Convention d'Istanbul afin de lutter contre la violence psychologique, le harcèlement et le harcèlement sexuel dans un contexte en ligne.[75]

- Inversement, la Convention d'Istanbul ne contient pas de dispositions spécifiques pour sécuriser les preuves électroniques dans les enquêtes nationales et internationales relatives à la violence en ligne contre les femmes. Les pays appliquant la Convention d'Istanbul devraient donc envisager de mettre en œuvre les pouvoirs procéduraux prévus aux articles 16 à 21 de la Convention de Budapest et de devenir parties à la Convention de Budapest pour faciliter la coopération internationale en matière de preuve électronique (articles 23 à 35 de la Convention de Budapest) concernant la violence en ligne contre les femmes.

[73] Voir Encourager la participation du secteur privé et des médias à la prévention de la violence contre les femmes et de la violence domestique : Article 17 de la Convention d'Istanbul https://rm.coe.int/16805970bd (lien vérifié le 13 septembre 2019). Cette publication ne représente pas nécessairement une position officielle du Conseil de l'Europe ou des Parties à la Convention d'Istanbul.
[74] https://www.coe.int/fr/web/genderequality/gender-equality-strategy
[75] Étant donné que la cyberviolence sexiste est un continuum de violence hors ligne, une approche holistique est nécessaire, couvrant toutes les dispositions de la Convention d'Istanbul plutôt que de se concentrer uniquement sur ces trois dispositions.

2.5 Examen d'autres réponses nationales et internationales

Les gouvernements ont adopté un large éventail de mesures juridiques et autres et la communauté internationale a adopté de nombreux instruments contraignants et non contraignants sur la protection des enfants et sur la violence contre les femmes ou la violence familiale (voir appendice). La plupart d'entre elles ne visent pas spécifiquement la cyberviolence, mais peuvent être appliquées hors et en ligne.

Les exemples suivants illustrent certaines des réponses nationales et internationales en matière de prévention, de protection, de poursuites et de criminalisation.[76]

2.5.1 Prévention

Les gouvernements, la société civile, le secteur privé et les organisations internationales prennent un large éventail d'initiatives - souvent en partenariat - pour prévenir la cyberviolence, comme en témoignent les exemples suivants.

L'Andorre a publié un Plan national de prévention de l'intimidation et du harcèlement à l'école 2016-2019, qui identifie quatre types de harcèlement, à savoir l'exclusion physique, verbale, sociale et cyberharcèlement, et des instruments détaillés de prévention.

L'Autriche, avec l'aide de l'Association des fournisseurs de services Internet (ISPA), a publié un livre d'information en allemand, anglais et arabe à l'intention des enfants afin de les sensibiliser aux risques liés à Internet.

En **France**, le Secrétariat d'État en charge de l'égalité entre les femmes et les hommes a publié pour les années 2017-2019 le *5ème plan de mobilisation et de lutte contre les violences*. Ce plan vise la poursuite de trois objectifs :[77]

- Sécuriser et renforcer les mécanismes mis en œuvre pour améliorer la trajectoire des femmes victimes de violence et garantir l'accès à leurs droits ;
- Renforcer l'action publique là où les besoins sont les plus grands ;
- Eradiquer la violence par la lutte contre le sexisme, qui banalise la culture de la violence et du viol.

Une partie de ce plan est consacrée à l'exposition aux contenus préjudiciables sur Internet, en particulier pour les jeunes femmes.

En **Allemagne,** le gouvernement soutient certaines initiatives dans ce domaine. Par exemple, en 2016, le 2e Congrès sur le cyberharcélement a été organisé sous les auspices du Ministère fédéral des affaires familiales, des personnes âgées, des femmes et de la jeunesse. Par ailleurs, l'association privée « Alliance contre le CyberHarcélement » est partenaire de la « Coalition pour la sécurité numérique » à l'initiative « Deutschland sicher im Netz » sous les auspices du Ministère fédéral de l'intérieur.

En **Italie,** le ministère de l'Éducation a lancé une campagne spécifique pour lutter contre la cyberintimidation, en créant un observatoire permanent pour chaque région d'Italie et en publiant

[76] En ce qui concerne la "protection des enfants contre l'exploitation et les abus sexuels facilités par les technologies de l'information et de la communication", voir également les réponses à un questionnaire des Parties à la Convention de Lanzarote dans le cadre du deuxième cycle de suivi par le Comité de Lanzarote. https://www.coe.int/en/web/children/2nd-monitoring-round

[77] - Sécuriser et renforcer les dispositifs qui ont fait leurs preuves pour améliorer le parcours des femmes victimes de violences et assurer l'accès à leurs droits ;
- Renforcer l'action publique là où les besoins sont les plus importants ;
- Déraciner les violences par la lutte contre le sexisme, qui banalise la culture des violences et du viol.

du matériel pédagogique (texte et multimédia) sur un site Web spécifique. Ce plan prévoyait notamment la mise en place d'un numéro d'urgence national doté d'un groupe de travail composé d'experts capables d'apporter la première aide en cas de cyberintimidation. Dans le cadre de cette campagne, un rôle important a été attribué à des mesures de réadaptation spécifiques, visant à sensibiliser l'auteur et sa famille aux conséquences de ses actes. Récemment, l'Italie a approuvé une loi spécifique pour lutter contre la cyberintimidation, et d'autres initiatives sont donc attendues dans les prochains mois.

Le **Japon** dispose d'un plan global appelé « Plan de base sur les mesures contre l'exploitation sexuelle des enfants »[78], qui comprend 88 mesures réparties en six piliers, à savoir :

- Sensibilisation du public à l'élimination de l'exploitation sexuelle des enfants, développement de la conscience sociale et renforcement de la collaboration avec la société internationale ;
- Appui aux enfants et aux familles pour assurer la croissance saine des enfants sans victimisation par l'exploitation sexuelle ;
- Promotion de mesures visant à prévenir l'apparition et la propagation de la victimisation, axées sur les outils utilisés pour l'exploitation sexuelle des enfants ;
- Protection rapide des enfants victimes et promotion d'un soutien approprié ;
- Renforcement des mesures de répression fondées sur la situation de victimisation et la réadaptation des délinquants ;
- Renforcement des fondements d'une société où les enfants ne seront jamais victimes d'exploitation sexuelle.

Maurice, le Conseil national de l'informatique a publié une directive sur les réseaux[79] sociaux et une brochure intitulée « Online Responsible Choices for Youngsters », qui est une campagne de sensibilisation sur la lutte contre la cyberintimidation et la cyberviolence, axée sur l'idée de respecter les droits des autres en ligne, notamment les droits de l'homme.

Le Mexique s'est doté d'une stratégie nationale de cybersécurité promue depuis 2017 par le Gouvernement fédéral et, conformément à cette stratégie, la Police fédérale a lancé une campagne nationale de prévention appelée « Cybersécurité Mexique » qui a touché directement plus de 680 000 citoyens et généré plus de 48 millions d'interactions dans les réseaux sociaux et les médias électroniques. Cette campagne vise à sensibiliser la société mexicaine à l'utilisation responsable des nouvelles technologies et d'Internet pour réduire les dommages causés par la cybercriminalité. Il comprend des journées d'information sur la cybersécurité contre l'exploitation sexuelle des enfants. En outre, depuis 2015, des Semaines nationales de la cybersécurité sont organisées en collaboration avec l'Organisation des États américains, dans le but de consolider les efforts de sensibilisation de la société mexicaine.

En **Norvège,** plusieurs initiatives publiques et privées ont été prises. Il s'agit notamment du service SlettMeg.no (« DeleteMe »), partiellement financé par l'État. Ce service a été lancé et était auparavant géré par l'Autorité norvégienne de protection des données, mais il est maintenant une entité distincte. Le service principal est un site Web qui a recueilli de l'information sur la façon d'entrer en contact avec divers services Internet et de médias sociaux pour faire retirer ou dissocier les contenus non désirés. SlettMeg.no offre également un service de réponse aux personnes qui ont des questions sur la façon de supprimer les contenus indésirables. Dans certains cas, SlettMeg.no a également aidé à contacter des prestataires de services. En outre, dans une affaire judiciaire récente, un conseiller principal de SlettMeg.no a témoigné en qualité de témoin expert au sujet de son expérience des effets et des conséquences des contenus privés non

[78] Voir http://www.npa.go.jp/safetylife/syonen/no_cp/measures/index_e.html (lien vérifié le 13 septembre 2019).
[79] http://cybersecurity.ncb.mu/English/Documents/Knowledge%20Bank/Guidelines/Guideline%20on%20Social%20Networks.pdf (lien vérifié le 13 septembre 2019).

désirés sur Internet, y compris les contenus à caractère sexuel. En plus du financement public, SlettMeg.no bénéficie également du soutien et de l'assistance d'une entreprise de télécommunications.

Barnevakten est une ONG qui se concentre sur l'information, les écoliers et leurs parents. L'une de leurs initiatives, « Bruk Hue » (« Utilisez votre tête ») est un projet de lutte contre le harcèlement sur Internet. Cela se fait en coopération avec d'autres organisations et est soutenu par plusieurs parties, dont une société de télécommunications et l'Autorité norvégienne des médias. En visitant les écoles, ce projet vise à sensibiliser les enfants et les jeunes à cette question et à les aider à faire de bons choix en ligne. Depuis 2009, ce projet a bénéficié à 1 000 écoles et a sensibilisé 250 000 enfants et 50 000 parents au harcèlement numérique et à la bonne conduite en ligne. Selon leurs propres statistiques, 7 enfants sur 10 disent, après la visite scolaire, qu'ils savent maintenant comment gérer le harcèlement numérique. 9 parents sur 10 disent qu'avant la visite scolaire, ils ne savaient rien de ce problème et/ou des solutions possibles.

L'Autorité norvégienne des médias gère également son propre projet, Trygg Bruk (« Utilisation sûre »), pour aider les enfants et les jeunes à mener une vie numérique plus sûre et meilleure. En coopération avec une ONG, il gère le Centre norvégien pour un Internet plus sûr (SIC Norvège). Ce centre est doté d'un conseil consultatif qui comprend des représentants de la police norvégienne, de ICT Norway, de l'Université d'Oslo et d'autres.

Singapour met l'accent sur la promotion du « cyber bien-être » dans le système éducatif. Le cyberbien-être (ou « Cyber Wellness » : CW) désigne le bien-être positif des utilisateurs d'Internet. Elle implique une compréhension du comportement en ligne et une prise de conscience de la façon de se protéger dans le cyberespace. Le Ministère de l'éducation utilise le cadre du cyberbien-être afin de développé l'instinct de l'enfant pour qu'il soit amené à protéger son propre bien-être dans le cyberespace et à lui donner les moyens d'assumer la responsabilité de son propre bien-être. L'enseignement relatif au cyberbien-être à Singapour comprend a) des leçons de cyberbien-être dans le programme scolaire formel et b) des programmes à l'échelle de l'école (p. ex. des conférences sur le cyberbien-être, des activités de cyberbien-être) pour renforcer l'importance de celui-ci et de ses messages. Les écoles sont guidées par le cadre du cyberbien-être pour planifier et mettre en œuvre un enseignement de celui-ci adapté au profil de l'élève et à l'environnement scolaire.

Le **Conseil de l'Europe** promeut la protection des enfants et leur autonomie dans un environnement numérique depuis de nombreuses années, notamment par le biais de l'actuelle « Stratégie du Conseil de l'Europe pour les droits de l'enfant »[80] qui affirme que les enfants :

> « ... ont le droit d'apprendre, de jouer et de communiquer en ligne - et d'être protégés contre les brimades, les discours de haine, la radicalisation, les abus sexuels et autres risques du « dark net». Garantir les droits de l'enfant dans l'environnement numérique est un défi majeur auquel tous les Etats membres du Conseil de l'Europe sont confrontés, et la Stratégie les aidera à fournir aux enfants des connaissances pratiques sur la manière d'être en ligne et de rester en sécurité. »

Une série de matériels éducatifs et de lignes directrices ont été mis à disposition.[81]

Le Conseil de l'Europe a déclaré le 18 novembre « Journée européenne pour la protection des enfants contre l'exploitation et les abus sexuels » et a centré l'édition 2017 sur « la protection des enfants contre l'exploitation et les abus sexuels facilitée par les technologies de l'information et

[80] http://www.coe.int/en/web/children/children-s-strategy
[81] http://www.coe.int/en/web/children/the-digital-environment#{"12440617" :[4]}

des communications (TIC) ». [82] Plusieurs tutoriels ont été mis à disposition concernant la sextorsion, l'envoi de sextos, les sollicitations sexuelles, le porno de vengeance et autres.

Le Conseil de l'Europe mène depuis 2012 une autre campagne d'éducation, intitulée « Mouvement contre le discours de haine[83] ». Cette campagne vise à lutter contre le racisme et la discrimination en ligne en mobilisant les jeunes et les organisations de jeunesse pour qu'ils reconnaissent et agissent contre ces violations des droits de l'homme. La campagne a été prolongée jusqu'à la fin de 2017 dans le cadre du Plan d'action du Conseil de l'Europe sur la lutte contre l'extrémisme violent et la radicalisation conduisant au terrorisme et poursuit les objectifs suivants :

- organiser des activités éducatives à l'intérieur et à l'extérieur des écoles sur la base du manuel des signets sur la lutte contre le discours de haine en ligne par l'éducation aux droits de l'homme ;
- reconnaître le discours de haine comme une violation des droits de l'homme et incorporer ce principe dans les programmes d'éducation aux droits de l'homme et à la citoyenneté ;
- mobiliser et coordonner avec les partenaires européens et nationaux ainsi qu'avec les services répressifs et les organes de contrôle nationaux les mesures prises pour lutter contre les discours de haine ;
- élaborer et diffuser des outils et des mécanismes de signalement des discours haineux, en particulier au niveau national ;
- promouvoir le 22 juillet comme Journée européenne des victimes de crimes motivés par la haine ;
- accorder une attention particulière aux discours de haine visant les réfugiés et les demandeurs d'asile, aux discours de haine sexistes et à l'antisémitisme, tout en tenant compte des causes profondes de l'extrémisme violent ;
- élaborer des contre-narratifs contre les discours haineux ;
- créer une plus grande coopération régionale pour soutenir les campagnes nationales ;
- soutenir la mise en œuvre des instruments pertinents du Conseil de l'Europe, tels que le guide « Droits de l'homme pour les internautes », la recommandation générale de la Commission européenne contre le racisme et l'intolérance sur la lutte contre le discours de haine et le Protocole additionnel à la Convention de Budapest sur la cybercriminalité sur la xénophobie et le racisme.

En ce qui concerne les discours haineux spécifiquement sexistes, une note d'information a été préparée par l'Unité de l'égalité des sexes du Conseil de l'Europe.[84]

L'article 9 de la Convention de Budapest couvre la pornographie mettant en scène de vrais enfants victimes, mais aussi des personnes paraissant mineures ainsi que des images réalistes (Morphée), c'est-à-dire des situations dans lesquelles un enfant réel n'est pas victime. L'exigence d'incriminer les actes connexes par le biais des articles 9.2.b et 9.2.c a donc une fonction de protection et vise à prévenir une « sous-culture favorisant la maltraitance des enfants ».[85]

L'article 25 de la directive 2011/93/UE de l'Union européenne du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants et la pédopornographie vise également à « faciliter la prévention et atténuer la victimisation secondaire ». Elle oblige les États membres de l'UE à retirer rapidement les matériels pédopornographiques sur leur territoire et à s'efforcer d'obtenir le retrait des matériels hébergés ailleurs. Il offre en outre la possibilité de

[82] https://www.coe.int/en/web/children/2017-edition
[83] Voir https://www.nohatespeechmovement.org/ (lien vérifié le 28 juillet dernier).
[84] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168059ad42)
[85] Voir le paragraphe 102 du Rapport explicatif sur la Convention de Budapest.

bloquer l'accès à la pédopornographie. En décembre 2016, la Commission européenne a publié une évaluation de l'application de l'article 25.[86]

La prévention des abus sexuels et de l'exploitation sexuelle est également l'un des objectifs de la Convention de Lanzarote (voir article 1 a) et chapitre II).

Le chapitre III de la Convention d'Istanbul couvre une série de mesures visant à prévenir la violence à l'égard des femmes et la violence familiale, allant de la promotion de changements dans les comportements sociaux à la sensibilisation et à l'éducation et aux programmes d'intervention préventive et de traitement.

2.5.2 Protection

Les mesures de protection sont souvent axées sur la protection des enfants contre l'exploitation et les abus sexuels. Par exemple, le chapitre IV de la **Convention de Lanzarote** comprend des mesures de protection et d'assistance aux victimes, exigeant des Parties qu'elles « établissent des programmes sociaux efficaces et mettent en place des structures multidisciplinaires pour apporter le soutien nécessaire aux victimes, à leurs proches parents et à toute personne qui est responsable de leur prise en charge ». Ces principes généraux doivent être réalisés afin :

- De veiller à ce que les obligations de confidentialité de certains professionnels appelés à travailler en contact avec la victime ne constituent pas un obstacle à leur signalement des abus sexuels ;
- D'encourager et de soutenir la mise en place de services d'information, tels que des lignes d'assistance téléphonique ou Internet, capables de garantir la confidentialité et l'anonymat des victimes ;
- D'assurer l'assistance aux victimes, à court et à long terme, dans leur rétablissement physique et psychosocial.

Depuis de nombreuses années, il existe des **lignes téléphoniques d'urgence** pour a) recevoir les plaintes pour maltraitance d'enfants et violence à l'égard des femmes et conduire à des enquêtes ou à la suppression de contenus, ou b) servir de lignes d'assistance téléphonique pour aider les victimes. À partir du milieu des années 1990, les lignes directes ont commencé à s'attaquer de plus en plus au matériel illégal sur Internet.

Plusieurs associations sont maintenant en activité en Europe, aux États-Unis, au Canada et dans d'autres pays qui promeuvent les bonnes pratiques, soutiennent le développement de nouvelles initiatives de lignes directes, échangent des rapports sur les matériels illicites et travaillent ensemble pour promouvoir la sensibilisation.

Les facteurs qui justifient la croissance rapide des lignes directes ont été décrits comme suit :[87]

- Internet est le « support idéal » pour les pédophiles parce qu' :
  - il permet aux personnes ayant le même intérêt de se réunir en ligne même si elles ne se connaissaient pas auparavant ;
  - il offre plusieurs méthodes de publication et d'échange d'images ;
  - il facilite l'organisation méticuleuse et le stockage des images ;
  - il permet aux enfants d'être contactés et attirés dans une relation en ligne ou hors ligne.

[86] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0872rom=EN
[87] Voir N. WILLIAMS, *The Contribution of Hotlines to Combating Child Pornography on the Internet*, disponible sur http://www.childnet.com/ufiles/combating-child-pornography.pdf (lien consulté le 13 septembre 2019).

- Internet a également provoqué le passage d'échanges privés d'images et de films non numériques à un transfert instantané de matériel sur un support facilement accessible à tous.

- Dans différents pays, la police s'est aperçue qu'une grande partie du matériel provenait de l'extérieur de sa juridiction, mais qu'il y était largement disponible.

- Des pressions sont exercées sur les politiciens pour qu'ils réagissent à ces menaces.

- Les internautes s'inquiètent d'un éventuel danger pour leur liberté d'expression, ils demandent donc une régulation équilibrée du phénomène et des garanties contre une surveillance déraisonnable.

Dans ce contexte, les lignes directes ont été considérées comme une approche appropriée parce qu'elles peuvent être créées sans modification de la législation, qu'elles peuvent fournir une première réponse aux plaintes du public et qu'elles peuvent participer activement à la conception des procédures de signalement des contenus illicites.

L'INHOPE (International Association of Internet Hotlines)[88] est un exemple de coopération entre les lignes directes nationales. Il s'agit d'un réseau d'associations qui se consacrent à la lutte contre les contenus et les activités criminellement illicites, en particulier en ce qui concerne le matériel pédopornographique, la manipulation en ligne et la haine en ligne, y compris la xénophobie.

En particulier, la plate-forme de signalement des matériels de maltraitance d'enfants présente une interface dans laquelle il est possible de choisir une localisation et d'être connecté à partir de celle-ci à la ligne directe locale d'un pays spécifique.

Certains pays, comme l'**Allemagne** et l'**Italie**, ont plus d'une association active sur le même sujet.

Au **Royaume-Uni**, une ligne directe a été créée et est gérée par le Child Exploitation and Online Protection Centre (CEOP) de l'Agence nationale du crime [89] qui permet à une personne, en quelques étapes simples, de signaler des situations potentiellement dangereuses, telles que des demandes d'images nues, des menaces en ligne, des demandes de rencontre en personne ou par webcam, la cyberintimidation, etc. Un conseiller en protection de l'enfance du CEOP peut offrir de l'aide pour assurer la sécurité de la victime éventuelle.

Aux **Pays-Bas,** la branche locale de la hotline INHOPE (Expertise centrum online misbruik kinderen ; Centre d'expertis en matière d'abus pédosexuels en ligne[90]) gère une véritable hotline, ainsi qu'un site web avec des informations et un chat associé, ou d'autres méthodes de contact appelés « help wanted ». "Ce site web est principalement dirigé contre la sextorsion et d'autres publications indésirables d'images souvent auto-générées.

En **Israël**, le Ministère de la sécurité publique, en collaboration avec la police israélienne, a récemment créé une unité spécialisée dans la lutte contre les infractions commises sur Internet contre les mineurs. La nouvelle unité, appelée « l'unité 105 », fonctionnera sur quatre niveaux différents : En premier lieu, l'unité comprend un centre d'appel national pour les délits mineurs ; en second lieu, l'unité comprend une unité spéciale d'enquête qui se concentrera sur la révélation et l'investigation des délits en ligne contre les mineurs ; en troisième lieu, l'unité participera à des activités dans les domaines de l'éducation, du bien-être et de la prévention du suicide des mineurs

[88] http://www.inhope.org/gns/home.aspx
[89] Voir le CEOP (Child Exploitation and Online Protection command) sur https://ceop.police.uk/safety-centre/ (lien vérifié le 13 septembre 2019).
[90] https://www.eokm.nl/

; en quatrième lieu, l'unité sera active en matière de retrait de contenu, lorsque celui-ci est nuisible aux mineurs (comme la « vengeance pornographie » ou les infractions au titre de la non publication des mandats de justice pour mineurs).

Certains plans nationaux prévoient également des actions ou des instruments pour protéger les victimes. En **France,** par exemple, l'un des objectifs[91] du plan français de lutte contre la violence prévoit la protection des victimes du cybersexisme par différentes actions :

- Faciliter le signalement des actes de cybersexisme ;
- Appliquer la nouvelle législation et ses sanctions aggravées en cas de cyberviolence sexuelle ;
- Distribuer un guide sur la cyberviolence sexuelle et les remèdes possibles.

Le Mexique a créé le Centre national d'attention aux cybercrimes contre les mineurs (CENADEM) au sein de la Division scientifique de la Police fédérale.

Le CENADEM est l'unité chargée de collaborer avec les autorités exécutives, fédérales et judiciaires, les acteurs sociaux, les institutions académiques et la société civile, à travers le suivi des rapports des citoyens, les arrêtés ministériels et judiciaires, la surveillance du réseau social public Internet et la coopération avec les organisations nationales et internationales afin de prévenir, rechercher et combattre la criminalité, ou les comportements antisociaux commis dans les médias électroniques, cybernétiques ou technologiques, liés au trafic humain ou à l'exploitation sexuelle des enfants. Cette unité reçoit les plaintes des citoyens par le biais d'une ligne directe de la police fédérale, le numéro de téléphone 088 est accessible dans tout le pays, pour soutenir les victimes de la cybercriminalité.

2.5.3 Poursuites judiciaires

Les cas fournis par les Parties et les observateurs à la T-CY (voir annexe) sont des exemples de poursuites réussies pour différents types de cyberviolence en Andorre, Autriche, Chili, France, Israël, Japon, Lettonie, Maurice, Pays-Bas, Philippines, Slovaquie, Slovénie et Etats-Unis.

L'âge est un critère décisif lorsqu'il s'agit de poursuivre les auteurs de cyberviolence. De nombreux États ont créé des unités spéciales chargées d'enquêter sur l'exploitation et les abus sexuels d'enfants en ligne et d'en poursuivre les auteurs.

C'est moins le cas si les victimes de cyberviolence sont des adultes.

Une exception peut être le « crime haineux ». Au **Royaume-Uni,** par exemple, le Crown Prosecution Service a publié des déclarations en août 2017 « sur la manière dont il entend poursuivre les crimes de haine et soutenir les victimes en Angleterre et au Pays de Galles ». Les crimes motivés par la haine sont définis comme suit :[92]

> La police et la SCP se sont entendues sur la définition suivante pour identifier et signaler les crimes haineux :
> « Toute infraction pénale qui est perçue par la victime ou toute autre personne comme étant motivée par l'hostilité ou un préjugé fondé sur la déficience réelle ou perçue d'une personne, la race ou la prétendue race, la religion ou la religion prétendue, l'orientation sexuelle ou l'orientation sexuelle prétendue ou une personne transgenre ou perçue comme étant transsexuelle ».

[91] Voir le 24ème Objectif du 5ème plan de mobilisation et de lutte contre les violences.
[92] https://www.cps.gov.uk/hate-crime

> Il n'y a pas de définition légale de l'hostilité, c'est pourquoi nous utilisons la compréhension quotidienne du mot, qui inclut la mauvaise volonté, le dépit, le mépris, les préjugés, l'hostilité, l'antagonisme, le ressentiment et l'aversion.

En 2015/2016, le CPS a poursuivi 15 442 crimes motivés par la haine, dont 84 % étaient des « crimes racistes et religieux aggravés ». Par rapport à l'année précédente, on constate une augmentation de 41 % des « crimes motivés par la haine à l'égard des personnes handicapées ».[93]

Le taux de condamnation est supérieur à 80 % :

> Plus de quatre crimes motivés par la haine poursuivis sur cinq aboutissent à une condamnation, ce qui est une bonne nouvelle pour les victimes. Plus de 73 % sont des plaidoyers de culpabilité, ce qui signifie qu'un plus grand nombre d'accusés plaident coupables en raison de la solidité de la preuve et de l'accusation, de sorte que les victimes n'ont pas à passer par le processus du procès.

Le CPS a publié des « guides de poursuites » sur les « crimes racistes et religieux haineux », les « crimes haineux homophobes, biphobes et transphobe »[94] et les « crimes haineux à l'égard des personnes en situation d'handicape ».[95]

2.5.4 Criminalisation de la cyberviolence

Alors que la plupart des États disposent d'une législation érigeant en infraction pénale les comportements liés à l'exploitation et aux abus sexuels d'enfants en ligne[96], la criminalisation d'autres formes de cyberviolence telles que la cyberintimidation, le harcèlement, la sextorsion et autres est un développement plus récent. Certaines lois incluent la responsabilité des fournisseurs de services. La plupart des États semblent appliquer le droit pénal ordinaire et d'autres dispositions. Par exemple :[97]

- **L'Autriche** érige en infraction pénale, au § 107c du Code pénal, le « harcèlement persistant impliquant des systèmes de télécommunication ou informatiques » :
  « (1) Toute personne qui, en utilisant un système de télécommunication ou un système informatique d'une manière qui peut causer une interférence déraisonnable avec le mode de vie de l'autre personne, de façon continue pendant une plus longue période 1. diffame une autre personne d'une manière qui peut être perçue par un plus grand nombre de personnes, ou 2. met des faits ou du matériel visuel sur sa sphère privée d'une autre personne à la disposition du plus grand nombre de personnes sans son consentement, encourt un emprisonnement pouvant atteindre un an ou une amende maximale de 720 euros.
  2) La personne est passible d'une peine d'emprisonnement pouvant aller jusqu'à trois ans si l'infraction aboutit au suicide ou à une tentative de suicide de la victime en vertu de l'al. 1."

[93] http://www.cps.gov.uk/news/latest_news/more_hate_crimes_prosecuted_by_the_crown_prosecution_service_than_ever_before/
[94] http://www.cps.gov.uk/legal/h_to_k/homophobic_and_transphobic_hate_crime/
[95] http://www.cps.gov.uk/legal/d_to_g/disability_hate_crime/
[96] Pour des exemples d'incrimination, voir Conseil de l'Europe/Division Protection des données et cybercriminalité (2012) : Protéger les enfants contre la violence sexuelle : les repères du droit pénal des Conventions de Budapest et de Lanzarote (Document de travail), Strasbourg, décembre 2012.
[97] Ce sont des exemples à titre d'illustration. Voir l'annexe pour plus d'informations sur la législation des Parties et des États observateurs.

- **Le Chili** a adopté en 2011 une « loi sur la violence à l'école » modifiant la loi générale sur l'éducation pour prévenir la violence psychologique et physique à l'école, y compris les brimades. La loi n'impose pas de sanctions pénales.

- En 2016, la **France** a adopté la loi sur la République numérique, qui prévoit une sanction plus sévère pour les personnes reconnues coupables de pornographie vengeresse. En vertu de la nouvelle législation, les auteurs de ces actes sont passibles d'une peine d'emprisonnement de deux ans ou d'une amende de 60 000 euros.

- **L'Allemagne** - comme beaucoup d'autres États - a recours à des dispositions du droit pénal qui ne sont pas spécifiques à l'environnement en ligne, comme l'article 238 du Code pénal allemand (harcèlement criminel), l'article 240 (recours à la menace ou à la force pour amener une personne à commettre, subir ou omettre un acte), l'article 241 (menace de commission d'un crime), l'article 176 (sévices à enfant) ou l'article 185 (insultes), Les articles 186 (diffamation), 187 (diffamation intentionnelle), 201 (atteinte à la vie privée de la parole) et 201a (atteinte à la vie privée intime par la photographie) du Code pénal allemand (*Strafgesetzbuch*) ainsi que l'article 33 de la loi sur le droit d'auteur relatif aux œuvres des arts visuels et à la photographie (*Kunsturhebergesetz*). L'article 238 (harcèlement criminel) inclut expressément la conduite au moyen de télécommunications (par. 1 no. 2) ou en utilisant les données personnelles d'une personne (par. 1 no. 3). Il en va de même pour l'article 176 (Maltraitance des enfants) qui couvre également expressément la conduite au moyen des télécommunications (par. 4, n° 3 et 4).
  La Loi visant à améliorer l'application de la loi dans les réseaux sociaux (en vigueur depuis juin 2017) vise à faire respecter les obligations de conformité pour les réseaux sociaux, mais n'étend pas la portée de la criminalisation. En particulier, les réseaux sociaux comptant plus de 2 millions d'utilisateurs enregistrés sont tenus d'assurer une gestion efficace des plaintes et de supprimer ou de bloquer les contenus illicites au regard de certaines dispositions du code pénal allemand dans un délai déterminé après avoir été informés de leur contenu. Cette obligation existe par exemple en ce qui concerne l'article 130 (incitation à la haine), l'article 241 (menace de commettre un crime), l'article 185 (insulte), l'article 186 (diffamation), l'article 187 (diffamation intentionnelle) et l'article 201a du Code criminel (violation de la vie intime en prenant des photographies).

- **Israël** applique également les dispositions du Code pénal et d'autres lois, telles que la loi sur la protection de la vie privée (1982) ou la loi sur la prévention du harcèlement sexuel (1998) pour les comportements en ligne. Par exemple, l'article 3 a) de la loi israélienne sur la prévention du harcèlement sexuel (1998) dispose qu'un harcèlement sexuel peut également être « la publication d'une image, d'une vidéo ou d'un enregistrement d'une personne, axée sur la sexualité de cette personne, lorsque la publication peut humilier ou dégrader cette personne, et lorsque cette personne n'a pas donné son consentement à cette publication ». La peine encourue pour ce comportement est de cinq ans d'emprisonnement et l'auteur est considéré comme un délinquant sexuel s'il est condamné. Cet article a été édicté principalement dans le but de s'attaquer au phénomène connu sous le nom de « pornographie de vengeance ». Habituellement, le phénomène comprend la documentation d'un acte sexuel qui a été commis avec le consentement de la personne concernée, puis une des personnes impliquées dans l'acte publie ce contenu sans le consentement de la deuxième personne. Ce « porno de vengeance » est considéré comme une sorte de cyberviolence envers la victime, et peut donc être considéré comme une forme de « cyberintimidation ».

- L'**Italie** a adopté en mai 2017 la loi n° 71/2017, intitulée « Règlement pour la protection des mineurs et la prévention et la lutte contre la cyberintimidation ». L'article 1 de la loi

définit la cyberintimidation comme « toute forme de pression psychologique, d'agression, de harcèlement, de chantage, de blessure, d'insulte, de dénigrement, de diffamation, de vol d'identité, d'altération, d'acquisition illicite, de manipulation, de traitement illicite des données personnelles des mineurs et/ou de diffusion par des moyens électroniques, y compris la distribution de contenu en ligne représentant également une ou plusieurs composantes de la famille du mineur dont le but intentionnel et prédominant est d'isoler un mineur ou un groupe de mineurs en mettant en œuvre un abus grave, une attaque malveillante ou un ridicule général et organisé ».

- **Le Japon** a adopté la loi anti-harcèlement qui couvre « le fait de faire des appels silencieux, d'appeler, de transmettre par télécopieur ou d'envoyer des messages texte par tout service de messagerie texte de façon persistante malgré ses rejets »..... « contre une personne, son conjoint, des parents en ligne directe ou des parents vivant ensemble ou toute personne ayant des liens étroits dans la vie sociale avec elle dans le but de satisfaire son affection, y compris ses sentiments romantiques, envers toute personne ou de satisfaire une rancune lorsque cette affection n'est pas partagée ». D'autres dispositions du Code pénal relatives à l'intimidation (art. 222, par. 19), à la contrainte (art. 223, par. 1), à la diffamation (art. 230, par. 1) ou aux insultes (art. 231) peuvent également être appliquées.

- **Le Liechtenstein** applique les dispositions de son Code pénal, telles que l'article 105 - Contrainte, l'article 106 - Contrainte aggravée, l'article 107 - Menace dangereuse, l'article 107a - Traque persistante, l'article 111 - Diffamation, l'article 112 - Fausse accusation, l'article 115 - Insulte, mais aussi les infractions contre les ordinateurs et les données.

- **La Slovaquie** n'a pas de dispositions spécifiques sur la « cyberviolence » mais applique un large éventail de dispositions du Code pénal telles que le harcèlement (article 360a du Code pénal), l'extorsion (article 189 du Code pénal), la contrainte (article 192 du Code pénal), l'exploitation sexuelle (article 201, article 201a, article 201b du Code pénal) et la diffamation (article 373 du Code pénal), l'atteintes aux droits d'autrui (art. 375, 376 du Code pénal), la fabrication de pornographie mettant en scène des enfants (art. 368 du Code pénal), la diffusion de pornographie mettant en scène des enfants (art. 369 du Code pénal), la possession de pornographie mettant en scène des enfants et la participation à des spectacles pornographiques impliquant des enfants, la corruption de la morale (art. 371, 372 du Code pénal), la Corruption de la morale des jeunes (article 211 du CC),l'Etablissement, le soutien et la promotion des mouvements visant à la suppression des droits et libertés fondamentaux (article 421 du CC), l'Expression de sympathie pour les mouvements visant à la suppression des droits et libertés fondamentaux (article 422 du CC), la Production, la distribution, la Possession de matériel extrémiste (articles 422a, 42 2b, 422c du Code pénal), la négation et approbation de l'Holocauste, des crimes contre l'humanité et des crimes politiques (article 422d du Code pénal), la diffamation de la nation, de la race et la condamnation (article 423 du Code pénal) ou l'incitation à la haine nationale, raciale et ethnique (article 424 du Code pénal).

- Au **Royaume-Uni,** en avril 2015, le partage de photographies ou de vidéos à caractère sexuel sans le consentement du sujet dans l'intention de causer de la détresse aux personnes ciblées est devenu une infraction pénale passible d'une peine d'emprisonnement maximale de deux ans. En septembre 2016, il a été annoncé que plus de 200 personnes avaient été poursuivies depuis l'entrée en vigueur de la loi.

- Les **États-Unis** criminalisent le « cyberharcèlement » dans 18 US Code Section 2261A(2) :
  « Qui que ce soit --
  (2) avec l'intention de tuer, blesser, harceler, intimider ou placer sous surveillance avec l'intention de tuer, blesser, harceler ou intimider une autre personne, utilise le courrier, tout service informatique interactif ou service de communication électronique ou système de communication électronique du commerce entre États, ou toute autre installation du commerce entre États ou étranger pour adopter une conduite qui --
  (A) fait raisonnablement craindre à cette personne la mort ou des lésions corporelles graves à une personne visée aux divisions (i), (ii) ou (iii) de l'alinéa (1)A) ; ou
  (B) cause, tente de causer ou risquerait vraisemblablement de causer à une personne visée aux sous-alinéas (i), (ii) ou (iii) de l'alinéa (1)A) un trouble émotif important,
  sera puni... »
  Les États-Unis ont également une disposition spécifique sur l' »extorsion impliquant des ordinateurs » (18 US Code Section 1030(a)(7)) qui inclut les menaces visant à causer des dommages à un ordinateur ou les menaces visant à obtenir des informations d'un ordinateur protégé.

En ce qui concerne la criminalisation de la cyberviolence, les observations suivantes peuvent être faites :

- Le droit interne seul ne suffit pas toujours, en particulier lorsque les délinquants commettent des crimes dans plusieurs pays, tentant de cacher leur identité et d'échapper à la capture. En général, la Convention de Budapest est susceptible d'être utile dans les enquêtes sur de nombreuses formes de cyberviolence, soit parce qu'une disposition de la Convention de Budapest incrimine un acte, soit parce que les dispositions procédurales de la Convention sont utiles pour la collecte de preuves ou la coopération internationale.

- En ce qui concerne la détermination de la peine, le Groupe sur la cyberviolence soupçonne que les pays ne punissent pas toujours la cyberviolence dans une mesure qui soit adaptée au préjudice causé. Elle a trouvé peu de données à l'appui de cette thèse ainsi que celle selon laquelle la cyberviolence n'est pas punie à un degré compatible avec les dommages physiques du monde, même si la victime subit des blessures extrêmes.[98] L'article 13 de la Convention de Budapest exige des pays qu'ils adoptent des sanctions effectives, proportionnées et dissuasives, y compris des peines privatives de liberté et des sanctions pécuniaires, le cas échéant. Cette norme devrait également s'appliquer aux poursuites pour cyberviolence lorsqu'elle constitue une infraction pénale.

- La Cour européenne des droits de l'homme a jugé, dans l'affaire K.U. c. Finlande,[99] que les États ont l'obligation de protéger leurs citoyens contre la criminalité, y compris les intrusions dans la vie privée. Les services répressifs ont donc l'obligation de mener des enquêtes et de poursuivre les auteurs d'actes de cyberviolence. Les États doivent prendre la cyberviolence au sérieux et veiller à ce que les lois soient modifiées, les compétences en matière d'enquête améliorées, etc.

- La cyberviolence cible de nombreuses personnes en fonction de leurs caractéristiques ou de leur appartenance à certains groupes. La législation du monde physique dans différents pays protège différents groupes sociaux et il ne serait pas possible d'énumérer toutes les bases sur lesquelles les personnes sont ciblées ou spécialement protégées.

[98] WITTES, Benjamin, " Closing the sextortion sentencing gap : a legislative proposal ", Brookings Institution, mai 2016, https://www.brookings.edu/research/closing-the-sextortion-sentencing-gap-a-legislative-proposal/ (lien consulté le 13 septembre 2019).
[99] Voir *K.U. c. Finlande* 02.12.2008 (Cour européenne des droits de l'homme, n° 2872/02).

Cependant, certaines bases familières sont : l'âge, la citoyenneté, la couleur, l'origine ethnique, la langue, l'état matrimonial, l'origine nationale, les défis physiques, la race, la religion, le sexe, l'orientation sexuelle et le statut social (ancien militaire, policier, réfugié et autres).[100] Les victimes peuvent bien sûr être ciblées pour plus d'une raison.

- Une grande partie de ce rapport est tout à fait pertinente et facilement extensible pour les victimes autres que les femmes et les enfants. Les attaques peuvent être similaires et les protections légales également disponibles ou inadéquates.

- Parce que la cyberviolence peut être liée ou entraîner des conséquences physiques, y compris des attaques physiques, les pays devraient veiller à ce que leurs lois en ligne et hors ligne soient harmonisées : les menaces électroniques peuvent être aussi terrifiantes que les menaces sur papier. En outre, les lois doivent être rédigées en termes technologiquement neutres tout en étant concises et différenciées. Au fur et à mesure que la criminalité électronique se développe, les lois rédigées avec souplesse seront les mieux à même d'y faire face.

[100] La cyberviolence touche également des personnes qui ne sont pas elles-mêmes les cibles - les parents d'enfants ciblés, par exemple.

3 Cyberviolence contre les femmes et les enfants : le rôle de la Convention de Budapest

3.1 Droit positif

Les articles 2 à 11 constituent la section de la Convention de Budapest consacrée à l'incrimination substantielle. Trois articles pourraient être utilisés en rapport avec la cyberviolence.[101] D'autres articles de fond érigent en infraction pénale les actes qui pourraient être liés à la cyberviolence, mais le lien est moins direct. De tels actes pourraient faciliter la violence et donner lieu à des poursuites, mais ils ne criminaliseraient pas la violence elle-même.

3.1.1 Articles ayant un lien plus direct avec la cyberviolence

- Article 4 - L'interférence des données dans un système critique peut entraîner la mort ou des blessures physiques ou psychologiques.
- Article 5 - L'interférence du système dans un système critique peut causer la mort ou des blessures physiques ou psychologiques.
- Article 9 - Pornographie enfantine. L'article 9, paragraphe 1, point a), érige en infraction pénale la production de pédopornographie destinée à la distribution électronique. La production de pornographie enfantine peut causer la mort et entraîne nécessairement des violences physiques et/ou psychologiques.

D'autres dispositions de l'article 9 couvrent la distribution d'images d'exploitation d'enfants ; cette distribution peut elle-même être source de violence psychologique. Il s'agit notamment de l'alinéa b) du paragraphe 1 de l'article 9, offrir ou mettre à disposition de la pornographie mettant en scène des enfants ; de l'alinéa c) du paragraphe 1 de l'article 9, distribuer ou transmettre de la pornographie mettant en scène des enfants ; et de l'alinéa d) du paragraphe 1, procurer de la pornographie mettant en scène des enfants à autrui (par exemple un enfant forcé de regarder l'exploitation d'un enfant).[102]

3.1.2 Articles ayant un lien facilitant avec la cyberviolence

La présente section donne des exemples, non exhaustifs, de la manière dont les actes susceptibles de faciliter la violence sont couverts par d'autres articles de la Convention de Budapest. L'expérience en matière d'application de la loi, les reportages dans les médias ou l'imagination pourraient facilement fournir d'autres exemples.

- Article 2 - l'accès illégal au système d'une victime est courant dans les cas de cybermenaces, de cyberharcèlement, de sextorsion et d'autres formes de violation de la vie privée équivalant à de la cyberviolence. Le système d'un tiers peut être accédé illégalement pour être utilisé comme plate-forme de messages ou d'attaques ou pour le vol de données intimes.

[101] Ces crimes pourraient viser n'importe quelle catégorie de personnes, pas seulement les femmes et les enfants. (L'article 9, paragraphe 2, point b), indique comment l'article 9 pourrait couvrir les hommes qui semblent être des enfants.

[102] Il est important de noter que la Convention de Lanzarote[Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Lanzarote, 27 octobre 2007)] est la principale source de droit pour ses Parties sur ce sujet et peut fournir des orientations aux non-Parties. D'autres instruments internationaux qui traitent de l'exploitation des enfants sont également importants.

- Article 3 - Le trafic entrant ou sortant peut être intercepté illégalement pour entraver la communication avec les services répressifs ou pour montrer à la victime que l'agresseur est au courant de tout ce que fait la victime. Le trafic peut également être intercepté pour commettre des atteintes à la vie privée équivalant à de la cyberviolence.

- Les articles 4 et 5 ont un lien direct avec la violence.

- Article 4 - l'interférence des données pourrait modifier les messages d'une personne sur les médias sociaux afin d'attirer l'hostilité.

- Article 5 - brouillage du système. Un agresseur qui envoie des menaces de mort peut prendre le contrôle suffisant d'un système informatique pour qu'une victime soit incapable de préserver les messages menaçants.

- Article 6 - mauvaise utilisation des dispositifs. Un criminel peut récupérer les mots de passe d'un système cible - une école, une organisation, etc. - d'utiliser son système interne pour transmettre les menaces.

- Article 7 - la falsification informatique peut être utilisée pour falsifier l'autorisation d'entrer dans un bâtiment.

- L'article 11 érige en infraction pénale la tentative, l'aide et la complicité de tout ou partie (selon les circonstances) des infractions visées aux articles 2 à 10. Il pourrait être utilisé pour lutter contre la cyberviolence en conjonction avec les articles 4, 5 et 9. Cependant, porter des accusations pour *tentative de* commettre l'un des autres crimes *facilitateurs* serait une méthode très indirecte pour lutter contre la violence.[103]

3.2 Droit procédural

L'article 14 dispose que les pays doivent appliquer les dispositions du droit procédural de la Convention de Budapest aux infractions substantielles visées dans la Convention, aux autres infractions pénales commises au moyen d'un système informatique et à la collecte de preuves sous forme électronique de toute infraction pénale.[104]

Les outils procéduraux sont donc disponibles pour poursuivre la cyberviolence sous toutes ses formes. Ces outils comprennent :

- la conservation accélérée (article 16) ;
- la conservation et la divulgation partielle (article 17) ;
- les ordonnances de production (article 18) ;
- les perquisition et saisie des données stockées (article 19) ;
- la collecte en temps réel des données relatives au trafic (article 20) ;
- l'interception des données relatives au contenu (article 21).

[103] Il en va de même pour l'inculpation de complicité.
[104] Les réservations limitées sont permises. Voir l'article 14.

3.3 Coopération internationale

L'article 23 exige des Parties qu'elles coopèrent dans toute la mesure du possible en vertu de tout instrument ou loi pertinente « aux fins d'enquêtes ou de procédures concernant des infractions pénales liées à des systèmes et données informatiques, ou pour la collecte de preuves sous forme électronique d'une infraction pénale ».

Les dispositions de la Convention de Budapest relatives à la coopération internationale comprennent :

- l'extradition (article 24) ;
- Les principes généraux de coopération (article 25) ;
- l'information spontanée (article 26) ;
- l'entraide judiciaire en l'absence d'accords internationaux (autres que la Convention de Budapest) (article 27) ;
- la confidentialité et les limites d'utilisation (article 28) ;
- la conservation accélérée (article 29) ;
- la divulgation accélérée des données relatives au trafic (article 30) ;
- assistance mutuelle pour l'accès aux données stockées (article 31) ;
- l'accès transfrontalier aux données stockées (article 32) ;
- l'assistance mutuelle dans la collecte en temps réel des données relatives au trafic (article 33) ;
- l'assistance mutuelle en matière d'interception des données relatives au contenu (article 34).

Certaines dispositions permettent l'application de la doctrine de la double incrimination ou incorporent le droit interne par référence. Que la double incrimination et le droit interne soient appliqués de manière rigide ou souple est particulièrement important dans les affaires de cyberviolence, car a) les affaires comportent souvent un élément transnational, et b) à ce jour, les pays n'ont pas systématiquement criminalisé des formes nouvelles et variées de cyberviolence.

3.3.1 Préservation

La préservation est l'outil le moins intrusif et le plus fondamental dans les enquêtes électroniques. Ainsi, l'article 29 ne permet pas aux Parties de refuser la conservation fondée sur la double incrimination, sauf dans des circonstances limitées. Si une Partie exige normalement la double incrimination pour rechercher, sécuriser ou divulguer des données stockées, elle peut également refuser de *conserver des* données si elle estime que la Partie requérante ne sera pas en mesure de satisfaire à la double incrimination lorsqu'elle demande la *divulgation* et si l'infraction concernée n'est pas visée aux articles 2 à 11. Toutefois, cela ne s'applique qu'aux Parties qui ont déposé une réserve concernant l'article 29.4.

Comme on l'a vu, la cyberviolence n'est que partiellement couverte par les articles 2 à 11. Pour que la préservation fonctionne dans ces cas, soit a) les Parties devraient appliquer la double incrimination avec souplesse, soit b) les Parties requérantes doivent demander la préservation sur la base de l'une des infractions facilitantes visées aux articles 2-7 et 11. Par exemple, une Partie peut demander la préservation dans une affaire de cybermenaces fondée sur l'article 2, soit l'accès illégal à l'ordinateur d'une victime.

3.3.2 Principes généraux de coopération

L'article 25 réitère dans un premier temps l'énoncé de l'article 23 selon lequel les Parties s'accordent l'entraide la plus large possible, y compris pour la collecte de preuves sous forme électronique d'une infraction pénale. L'article 25 déclare ensuite que, lorsqu'une Partie évalue la double incrimination, elle doit se demander si le comportement qui sous-tend l'infraction pour

laquelle l'assistance est demandée est une infraction pénale au regard de sa propre législation. La Partie n'est pas autorisée à se concentrer sur la question de savoir si l'infraction relève de la même catégorie d'infractions, ou si elle est appelée par le même nom, que dans le droit interne. L'article met l'accent sur la flexibilité pour que de nouveaux crimes puissent être poursuivis.

3.3.3 Assistance mutuelle pour l'accès aux données stockées

L'article 31 incorpore par référence certains « instruments, arrangements et lois internationaux », ainsi que « les autres dispositions pertinentes du présent chapitre ». L'incorporation par référence de ces instruments, arrangements, lois et autres dispositions peut signifier que la double incrimination ou le droit interne peut affecter la coopération dans les affaires de cyberviolence.

3.3.4 Assistance mutuelle pour la collecte en temps réel des données relatives au trafic et assistance mutuelle pour l'interception des données relatives au contenu

Les articles 33 et 34 reprennent le droit interne dans leurs termes. En vertu de l'article 33, les Parties doivent collecter des données relatives au trafic les unes pour les autres en temps réel « au moins en ce qui concerne les infractions pénales pour lesquelles[une telle collecte] serait disponible dans une affaire nationale similaire ». L'article 34 fait obligation aux Parties de collecter ou d'enregistrer des données relatives au contenu « dans la mesure permise par la législation nationale... ».

La législation nationale actuelle d'un pays peut ne pas couvrir les infractions de cyberviolence en soi. Si tel est le cas, l'État requis peut être en mesure d'extraire des éléments de la demande de l'État requérant pour pouvoir coopérer. Par exemple, un pays peut s'appuyer sur le fait que les menaces ont été envoyées sans tenir compte du fait qu'elles l'ont été par voie électronique. Neanmoins, si le droit interne ne couvre pas une infraction en soi et si des éléments utilisables ne peuvent être extraits d'une demande LBA, la coopération internationale pour obtenir des données relatives au trafic ou au contenu peut être bloquée.

3.4 La question d'une note d'orientation

Trois des dispositions de fond de la Convention de Budapest ont un lien direct avec la cyberviolence. D'autres dispositions couvrent les comportements (payants) susceptibles de faciliter de tels actes de violence. Les outils procéduraux s'appliqueraient dans les deux cas. Les outils de coopération internationale de la Convention s'appliqueraient également dans tous les cas, mais plusieurs de ces outils importants pourraient être entravés par la doctrine de la double incrimination ou par le droit interne.

Une note d'orientation T-CY pourrait expliquer ce qui précède. Toutefois, il se peut qu'elle n'offre qu'une solution partielle. Il semblerait donc souhaitable d'envisager de donner des orientations sur la manière dont la Convention de Budapest et son Protocole sur la xénophobie et le racisme pourraient être appliqués conjointement avec la Convention d'Istanbul et de Lanzarote, plutôt que de rédiger une note d'orientation sur les dispositions de la Convention de Budapest comme telles.

4 Constatations et recommandations

4.1 Constatations (lacunes et problèmes)

4.1.1 Sur le concept de cyberviolence

La cyberviolence peut être définie provisoirement comme :

> l'utilisation de systèmes informatiques pour causer, faciliter ou menacer de causer à des personnes de la violence qui leur cause ou est susceptible de leur causer un préjudice ou des souffrances physiques, sexuelles, psychologiques ou économiques et qui peut comprendre l'exploitation de leur situation, de leurs caractéristiques ou de leur vulnérabilité.

Cela comprend le cyberharcèlement (y compris la cyberintimidation), les formes de violation de la vie privée, l'exploitation sexuelle en ligne et l'abus sexuel des enfants. Certaines formes de cybercriminalité ainsi que les menaces directes ou la violence réelle peuvent également constituer de la cyberviolence.

Les formes de cyberviolence peuvent représenter des violations des droits de l'homme et des formes de discrimination.

Le concept de cyberviolence tel qu'il est utilisé dans cette étude reste insaisissable et difficile à délimiter. D'autres recherches sont nécessaires pour arriver à un concept mûr de la cyberviolence.

4.1.2 Cyberviolence : Portée, impact et enjeux

La cyberviolence est une violence à l'encontre d'individus avec des conséquences souvent dévastatrices pour les individus. Si les conséquences de la cyberviolence ne sont pas toujours assimilées aux conséquences de la violence physique, la cyberviolence devrait être une préoccupation majeure pour les sociétés.

De nombreuses formes de violence aujourd'hui associées à la cyberviolence, dans leur manifestation physique, ont toujours été des problèmes auxquels les sociétés ont dû faire face, entre autres, par le droit pénal (coercition, menaces, fausses accusations, insultes, diffamation, harcèlement, extorsion, violation de la vie privée, viol, etc.)

Les solutions matérielles à la violence peuvent donc aussi s'appliquer aux actes de violence si des ordinateurs sont utilisés.

Cependant :

- Alors que la violence physique dans le monde est normalement limitée par la nécessité d'une interaction face à face, ou par les limites des moyens de communication plus traditionnels, il y a peu d'obstacles à la cyberviolence commise par le biais des systèmes informatiques. En particulier, les médias sociaux et l'augmentation considérable de la collecte, de la disponibilité publique et de la facilité de recherche de l'information ont facilité la prolifération de la cyberviolence. Dans le monde physique, il serait impossible de recruter des centaines d'hommes pour aller dans la maison d'une ex-petite amie afin d'exiger un acte sexuel. Il est tout à fait possible d'organiser cela via le Net.

- La cyberviolence n'est pas simplement une extension de la violence physique dans le monde. La nature et l'impact de la violence semblent avoir changé si elle est commise au moyen de systèmes informatiques. Des solutions spécifiques sont donc nécessaires.

La cyberviolence peut comprendre de nouvelles formes de violence qui n'ont pas d'équivalent dans le monde physique, ou qui nécessitent une criminalisation plus cohérente dans différents États pour permettre une coopération internationale.

Il se peut qu'aucun crime du monde physique ne se répète ou ne persiste après sa perpétration sans que le criminel n'agisse, pourtant c'est le cas de nombreuses formes de cyberviolence. Une fois que le matériel a été affiché, copié, redistribué, etc, les souffrances de la victime se poursuivent, bien que le criminel n'ait pas besoin de prendre des mesures. Cet aspect de la cyberviolence semble souvent ne pas se refléter dans la détermination de la peine des délinquants, alors que les effets néfastes de la cyberviolence sur les victimes peuvent être essentiellement de longue durée. Ils sont victimes d'une nouvelle victimisation chaque fois qu'un nouveau collègue professionnel, un partenaire romantique, un futur beau-parent ou quelqu'un d'autre fait des recherches en ligne sur eux.

4.1.3 Réponses nationales et internationales à la cyberviolence

Les gouvernements, la société civile, le secteur privé et les organisations internationales adoptent de plus en plus de politiques et de mesures pour lutter contre la cyberviolence. L'accent est mis principalement sur la prévention et l'éducation des enfants et des jeunes adultes.

Les mesures de protection sont souvent axées sur la protection des enfants contre l'exploitation et les abus sexuels. Les lignes directes jouent un rôle important à cet égard.

Des unités spécialisées dans les enquêtes et les poursuites concernant les abus sexuels d'enfants sur Internet ont été créées dans un certain nombre d'États.

Cependant, cela semble être moins le cas en ce qui concerne les autres formes de cyberviolence.

De nombreux États ont érigé en infraction pénale les formes de coercition, les menaces, le harcèlement (sexuel), les atteintes à la vie privée, les insultes, l'extorsion et d'autres formes de violence, notamment la xénophobie, le racisme et d'autres formes de discours de haine qui peuvent également être utilisées lorsque des systèmes informatiques sont utilisés. Certaines formes de cyberviolence peuvent être inculpées en vertu de ces lois et d'autres lois issues du monde physique (incitation à commettre un crime, par exemple).

Outre l'incrimination des actes liés à l'exploitation et aux abus sexuels concernant des enfants, les dispositions juridiques spécifiques concernant d'autres formes de cyberviolence sont moins courantes. Certains États indiquent qu'ils ont criminalisé la cyberharcèlement et la cyberintimidation.

La réponse du droit pénal à des formes spécifiques de cyberviolence est donc limitée pour différentes raisons, notamment parce que les réponses du droit pénal ne sont pas toujours considérées comme appropriées et que d'autres solutions peuvent être préférables.

Plusieurs problèmes ont été relevés :

- Les victimes de cyberviolence ne savent souvent pas quoi faire pour obtenir de l'aide.
- Les autorités chargées de l'application de la loi ne sont souvent pas en mesure d'aider les victimes et la cyberviolence peut ne pas être considérée comme une priorité en matière d'application de la loi ou ne pas être considérée comme suffisamment grave (« nous ne faisons pas de plaintes Facebook »).

- S'il existe des solutions à la violence en ligne, en particulier l'abus sexuel à l'encontre des enfants, il existe des lacunes en ce qui concerne les réponses à la violence en ligne contre les adultes.

- Les fournisseurs de médias sociaux peuvent jouer un rôle dans la prévention et le contrôle de la cyberviolence et dans la protection des victimes. Ce rôle est souvent considéré comme insuffisant.

- La prévention et le contrôle de la cyberviolence peuvent aller à l'encontre de la liberté d'expression et d'autres droits (par exemple, la liberté d'expression contre le discours haineux). Lorsqu'ils ne sont pas en conflit, leur relation doit tout de même être examinée avec soin.

4.1.4 Types de cyberviolence abordés ou non dans les accords internationaux

- L'**exploitation sexuelle et les abus sexuels d'enfants en ligne** sont couverts par la Convention de Lanzarote (STCE 201) qui s'applique également si elles sont commises au moyen de systèmes informatiques (TIC). Toutefois, étant donné que ce traité ne dispose pas de pouvoirs procéduraux et de moyens de coopération internationale spécifiques pour les enquêtes informatiques et l'obtention de preuves électroniques, ses Parties devraient être informées des outils et moyens offerts par la Convention de Budapest et encouragées à les utiliser pour traiter efficacement la cyberdimension de l'exploitation sexuelle et des abus sexuels concernant des enfants. A cette fin, les Parties à la Convention de Lanzarote qui n'ont pas encore ratifié la Convention de Budapest devraient le faire.

- **La cybercriminalité**, c'est-à-dire les atteintes à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques et certaines infractions commises au moyen d'ordinateurs, peuvent causer un préjudice ou des souffrances physiques, sexuelles, psychologiques ou économiques à des personnes et sont traitées par la Convention de Budapest sur la cybercriminalité en termes de droit pénal matériel, complétées par des pouvoirs de procédure et de coopération internationale pour enquêter et poursuivre des crimes pouvant constituer, dans certains cas, une cyberviolence. Toutefois, les sanctions et les mesures ne sont pas toujours proportionnelles dans la pratique à l'impact sur les individus. La cybercriminalité peut également faciliter d'autres types de cyberviolence.

- **Les crimes motivés par la haine** sont partiellement couverts par le Protocole additionnel à la Convention de Budapest sur la xénophobie et le racisme et concernent donc la cyberviolence motivée par certains préjugés, mais pas par d'autres caractéristiques telles que le sexe, l'orientation sexuelle ou le handicap. Les travaux du Conseil de l'Europe et d'autres organisations sur la discrimination et l'intolérance sont également pertinents. Les questions clés sont le rôle des fournisseurs de services et la question du discours haineux par opposition à la liberté d'expression.

- **Les menaces directes et la violence physique** couvrent un large éventail de comportements couverts par le droit interne de la plupart des États et devraient également s'appliquer si elles sont commises au moyen d'ordinateurs. Là encore, les mécanismes de la Convention de Budapest peuvent être utilisés pour les enquêtes nationales et internationales. De telles menaces directes ou de telles violences peuvent donner lieu à une réponse proportionnée de la justice pénale.

- **Les atteintes à la vie privée** impliquent toute une série de comportements qui peuvent être partiellement traités par la Convention de Budapest et d'autres traités (par exemple, l'article 34 de la Convention d'Istanbul - Traque). Il n'est pas toujours évident

qu'une telle conduite débouche sur une réponse suffisante de la justice pénale et que les victimes recevront l'assistance nécessaire.[105] Davantage d'orientations pourraient aider les États à appliquer les dispositions existantes de manière efficace et adéquate pour lutter contre ce type de cyberviolence. D'autres recherches seraient nécessaires pour déterminer si l'application des dispositions existantes est suffisante.

- **Le cyberharcèlement** est la catégorie la plus large de cyberviolence et comprend, entre autres, la cyberintimidation. La Convention d'Istanbul traite de la « violence psychologique » à l'article 33 et du « harcèlement sexuel » à l'article 40, et ces concepts pourraient également être appliqués à la cyberviolence[106]. Il en va peut-être de même pour les dispositions relatives à la violence et à la discrimination à l'égard des femmes dans les traités, résolutions et déclarations internationaux. De nombreuses dispositions couvrant les formes de violence dans le droit interne s'appliqueraient également à la cyberviolence. Toutefois, même si ces solutions peuvent être une source d'inspiration, elles ne semblent pas répondre de façon satisfaisante aux particularités du cyberharcèlement.

4.1.5 Rôle de la Convention de Budapest

La Convention de Budapest, par le biais d'un certain nombre de dispositions de droit pénal positif, aborde directement certains types de cyberviolence. D'autres dispositions concernent les actes facilitant la cyberviolence.

Les pouvoirs procéduraux et les dispositions de la Convention sur la cybercriminalité relatives à la coopération internationale aideront à enquêter sur la cyberviolence et à obtenir des preuves électroniques.

La Convention de Budapest et les traités tels que les Conventions d'Istanbul et de Lanzarote se complètent mutuellement.

Il semble que l'on pourrait faire davantage pour souligner cette complémentarité et promouvoir les synergies entre ces trois instruments.

4.2 Recommandations

Des efforts - y compris des mesures conjointes - de la part d'un large éventail de parties prenantes sont nécessaires pour s'attaquer au problème multiforme de la cyberviolence.

Au niveau du Comité de la Convention du Conseil de l'Europe et de la Convention sur la cybercriminalité :

Rec1 Le Conseil de l'Europe (Secrétariat T-CY et C-PROC) devrait envisager de mettre à disposition des informations en ligne sur la cyberviolence incluses dans la présente étude sur les politiques, stratégies et mesures de prévention, de protection et de justice pénale prises par le secteur public, la société civile et les organisations du secteur privé, et créer un portail en ligne pour recevoir, documenter et rendre disponibles les nouveaux développements et informations sur ces politiques, stratégies et mesures prises par les organisations du secteur public, la société civile et le secteur privé.

Rec 2 Compte tenu de la différence de portée mais aussi de la complémentarité entre la Convention de Budapest et son Protocole, et les Conventions de Lanzarote et d'Istanbul,

[105] Une intervention du système de justice pénale n'est pas toujours nécessaire.
[106] Il pourrait être utile d'étudier comment les Parties à la Convention d'Istanbul ont appliqué ces dispositions.

les Parties[107] - dans le cadre de leurs obligations conventionnelles respectives - et le Secrétariat pourraient envisager de promouvoir des synergies entre ces instruments dans la pratique, notamment en :

- sensibiliser les Parties aux dispositions de ces traités ;
- en s'inspirant de ces traités dans les activités de renforcement des capacités et lors de la fourniture de conseils aux pays ;
- encourager les Parties aux Conventions de Lanzarote et d'Istanbul à introduire les pouvoirs procéduraux des articles 16 à 21 de la Convention de Budapest dans leur droit interne et à envisager de devenir Parties à la Convention de Budapest pour faciliter la coopération internationale en matière de preuve électronique (articles 23 à 35 de la Convention de Budapest) en relation avec la violence sexuelle contre les enfants en ligne et la violence contre les femmes et la violence familiale ;
- encourager les Parties à la Convention de Budapest à s'inspirer des articles 33, 34 et 40 de la Convention d'Istanbul pour lutter contre la violence psychologique, le harcèlement et le harcèlement sexuel en ligne et de la Convention de Lanzarote - en particulier des articles 18 à 23 - pour lutter contre l'exploitation sexuelle et les abus sexuels des enfants en ligne, et à envisager de devenir parties à ces traités.

Rec 3 Les Parties à la Convention de Budapest devraient envisager d'améliorer la formation et la sensibilisation des autorités de justice pénale en matière de cyberviolence, y compris les enquêtes, les poursuites et les sanctions, lorsqu'elle constitue une infraction pénale. Le Conseil de l'Europe - par l'intermédiaire de son C-PROC - et d'autres organisations devraient soutenir ces activités de renforcement des capacités. Les membres de T-CY souhaiteront peut-être partager la présente étude avec les institutions compétentes de leur pays.

Rec. 4 Les mesures visant à prévenir la cyberviolence, à la protéger contre et - dans les cas où elle constitue une infraction pénale - à en poursuivre les auteurs devraient être conçues comme contribuant à la mise en œuvre de l'Agenda 2030 des Nations Unies pour le développement durable,[108] en particulier l'objectif 16 du développement durable.

Rec 5 Les Parties à la Convention de Budapest devraient assurer un meilleur équilibre entre les sexes dans les institutions qui s'occupent de la cybercriminalité.

4.3 Suivi du dossier

Le T-CY devrait envisager de donner suite à ces recommandations dans les 24 mois suivant leur adoption.

[107] Ayant à l'esprit que toutes les Parties à la Convention de Budapest ne sont pas Parties aux Conventions d'Istanbul et de Lanzarote.

[108] http://www.un.org/sustainabledevelopment/peace-justice/
Objectif 16 : « Promouvoir des sociétés pacifiques et inclusives pour le développement durable, assurer l'accès de tous à la justice et mettre en place des institutions efficaces, responsables et inclusives à tous les niveaux », notamment :

- une réduction significative de toutes les formes de violence et des taux de mortalité qui y sont liés, partout dans le monde ;
- la fin des mauvais traitements, de l'exploitation, de la traite et de toutes les formes de violence et de torture à l'égard des enfants ;
- l'état de droit aux niveaux national et international et l'égalité d'accès à la justice pour tous ;
- des institutions efficaces, responsables et transparentes à tous les niveaux ;
- une prise de décisions réceptive, inclusive, participative et représentative à tous les niveaux ;
- renforcé les institutions nationales compétentes, notamment par la coopération internationale, pour renforcer les capacités à tous les niveaux afin de prévenir la violence et de combattre le terrorisme et la criminalité ;
- des lois et des politiques non discriminatoires en faveur du développement durable.

5 Annexe

5.1 Références/sources/bibliographie

APC Countries report for the project "From impunity to justice" as a part of the project "End violence: Women's right and safety online"
http://www.genderit.org/onlinevaw/countries/
Other links to materials http://genderit.org/onlinevaw/about/ (links last checked on March 29, 2017).

CCSO Cybercrime Working Group (2013): Cyberbullying and the Non-consensual Distribution of Intimate Images. Report to the Federal/Provincial/Territorial Ministers Responsible for Justice and Public Safety (Canada). June 2013.
http://www.justice.gc.ca/eng/rp-pr/other-autre/cndii-cdncii/pdf/cndii-cdncii-eng.pdf (links last checked on March 29, 2017).

Citizen Lab (2017): Submission of Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Special Rapporteur on violence against women, its causes and consequences, Ms. Dubravka Šimonović.
https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf

CITRON, Danielle K. (2017): Addressing Cyber Harassment: An Overview of Hate Crimes in Cyberspace. University of Maryland Francis King Carey School of Law Legal Studies Research Paper, No. 2017-9.

CLARK, Marilyn/GRECH, Anna (2017): Journalists under Pressure. Unwarranted interference, fear and self-censorship in Europe. Council of Europe Publishing. Strasbourg.

COUNCIL OF EUROPE (2007): Eliminating corporal punishment (A human rights imperative for Europe's children). Strasbourg. ISBN 978-92-871-6182-6.

COUNCIL OF EUROPE (2008): Protecting children from sexual violence (A comprehensive approach). Strasbourg. ISBN: 978-92-871-6972-3.

COUNCIL OF EUROPE (2008): Eradicating violence against children. Strasbourg. ISBN: 978-92-871-6432-2.

COUNCIL OF EUROPE (2016): Encouraging the participation of the private sector and the media in the prevention of violence against women and domestic violence: article 17 of the Istanbul Convention. Strasbourg

COUNCIL OF EUROPE (2017): Bullying: perspectives, practice and insights. Strasbourg

COUNCIL OF EUROPE/DATA PROTECTION AND CYBERCRIME DIVISION (2012): Protecting children against sexual violence: the criminal law benchmarks of the Budapest and Lanzarote Conventions (Discussion paper), Strasbourg, December 2012.

CROWN PROSECUTION SERVICE. Violence against Women and Girls. Crime Report 2015-16.

DALLA POZZA, Virginia; DI PIETRO, Anna; MOREL, Sophie and PSAILA, Emma (2016): Cyberbullying among Young People. Directorate-General for Internal Policies - Policy Department C: Citizens' Rights and Constitutional Affairs. Study for the LIBE Committee.
http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf (link last checked on March 29, 2017)

DE VIDO, Sara (2016): Donne, violenza e diritto internazionale. La Convenzione di Istanbul del Consiglio d'Europa 2011, 2016, 289 pp., ISBN: 978857536811.

ECKERTOVÁ, Lenka; DOČEKAL, Daniel (2013): Bezpečnost dětí na Internetu (Safety of children in Internet) Praha: Albatros Media, 2013. 224 p., portr. ISBN: 978-80-251-3804-5.

EIGE, "Cyberviolence against women and girls",
http://eige.europa.eu/sites/default/files/documents/cyber_violence_against_women_and_girls.pdf

EL ASAM AIMAN; SAMARA MUTHANNA (2016): Cyberbullying and the law: A review of psychological and legal challeng. Computers in Human Behavior 65 (2016) 127-141.

ERNI, John Nguyet (2014): Sex/Text: Internet Sex Chatting and "Vernacular Masculinity" in Hong Kong. International Proceedings of Economics Development and Research, Vol. 44.
European Union Agency for Fundamental Rights. Violence against women: an EU-wide survey. (2014)
http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report (link last checked on March 29, 2017)

FEMINISM IN INDIA.COM, ""Violence" Online In India: Cybercrimes Against Women & Minorities on Social Media"
https://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf

FRYLING, Meg; RIVITUSO, Giacomo (2013): Investigation of the Cyberbullying Phenomenon as an Epidemic (2013)

GÁLIK, Slavomír (2014): Možnosti a nebezpečenstvá komunikácie na internete (Possibilities and dangers of online communication).Trnava: Univerzita sv. Cyrila a Metoda, Fakulta masmediálnej komunikácie, 2014. 165 p. ISBN: 978-80-8105-605-5.

GARDINER, Adelle (2012): The online behaviour of children and young people - Preliminary review of literature. Study for the Scotland's Commissioner for Gender and Young People (2012).
http://www.cypcs.org.uk/downloads/Adult%20Reports/Online_behaviour_desktop_review_2012.pdf (link last checked on March 29, 2017)

GLEESON, Helen (2014): The Prevalence and Impact of Bullying linked to Social Media on the Mental Health and Suicidial Behaviour Among Young People. Literature review commissioned by HSE National Office for Suicide Prevention and Dept. of Education and Skills.
https://www.education.ie/en/Publications/Education-Reports/The-Prevalence-and-Impact-of-Bullying-linked-to-Social-Media-on-the-Mental-Health-and-Suicidal-Behaviuor-Among-Young-People.pdf (link last checked on March 29, 2017)

Global Fund for Women. Online violence: Just because it's virtual doesn't make it any less real.
https://www.globalfundforwomen.org/online-violence-just-because-its-virtual-doesnt-make-it-any-less-real/ (link last checked on March 29, 2017)

GREGUSSOVÁ, Monika; DROBNY, Miroslav (2013): Deti v sieti (Children in the web) 2013. eSlovensko. 111 p. ISBN: 978-80-970676-6-3.

AL-ALOSI, HADEEL (2017): Cyber-violence: Digital abuse in the context of domestic violence. In: University of New South Wales Law Journal, The, Vol. 40, No. 4, 2017: 1573-1603.

HENRY, Nicola; POWELL, Anastacia (2016): Technology-Facilitated Sexual Violence - A Literature Review of Empirical Research.
[See also the references related to this publication at

http://journals.sagepub.com/doi/abs/10.1177/1524838016650189]

HINDUJA, Sameer and PATCHIN Justin W. Cyberbullying.org (2016): Description of State Cyberbullying Laws and Model Policies (U.S. based study, 2016)
http://cyberbullying.org/Bullying-and-Cyberbullying-Laws.pdf

Cyberbullying Data (2016)
http://cyberbullying.org/2016-cyberbullying-data (links last checked on March 29, 2017)

HOLÍKOVÁ, Barbora; MADRO, Marek (eds.) (2015): Virtuálna generácia (Virtual Generation). Bulletin of the Conference "Virtual Generation". Bratislava. ISBN: 978-80-971933-2-4.

HOLLEY, Peter (2015): Afghan women say hackers and threats have made them afraid of Facebook. The Washington Post, 18 September 2015.
https://www.washingtonpost.com/world/afghan-women-say-hackers-and-threats-have-made-them-afraid-of-facebook/2015/09/16/b5ee441e-5af3-11e5-8475-781cc9851652_story.html?utm_term=.b365cc71bf68 (link last checked on March 29, 2017)

HUDECOVÁ, Anna; KURČÍKOVÁ, Katarína (2014): Kyberšikanovanie ako rizikové správanie (Cyberbullying as risk behaviour). Banská Bystrica: Belianum, Univerzita Mateja Bela v Banskej Bystrici, 2014. 115 p. ISBN: 978-80-557-0745-7.

Insafe Helplines (EU based network of helplines for children and young people online issues)
https://helplines.betterinternetforkids.eu/ (link last checked on March 29, 2017)

Internet Governance Forum (IGF) (2015): Best Practice Forum (BPF) on Online Abuse and Gender-Based Violence Against Women Online (2015)
http://www.intgovforum.org/cms/documents/best-practice-forums/539-draft-jp-bpf-women/file
(link last checked on March 29, 2017)

INTERNATIONAL WOMEN'S MEDIA FOUNDATION'S REPORT Violence and Harassment against Women in the News Media: A Global Study (2014) http://www.iwmf.org/wp-content/uploads/2014/03/Violence-and-Harassment-against-Women-in-the-News-Media.pdf

LANGOS, Colette (2012): Cyberbullying: The Challenge to Define. Cyberpsychology, Behavior, and Social Networking, Volume 15, Number 6, 2012.
https://ssrn.com/abstract=2361267 (link last checked on March 29, 2017)

LENHART, Amanda; YBARRA, Michele; ZICKUHR, Kathryn, and PRICE-FEENEY, Myeshia (2016): Online Harassment, Digital Abuse, and Cyberstalking in America. Data and Society Research Institute, Center for Innovative Public Health Research. 21 November 2016, https://innovativepublichealth.org/publications/online_harassment_2016/ (link last checked on April 6, 2017).

LEVI, Nathaniel; CORTESI, Sandra; GASSER, Urs; CROWLEY, Edward; BEATON, Meredith; CASEY, June; NOLAN, Caroline (2012): Bullying in a Networked Era: A Literature Review. Berkman Klein Center Research Publication No. 2012-17
https://ssrn.com/abstract=2146877 (link last checked on March 29, 2017)

LEWIS, Ruth; ROWE, Michael; WIPER, Clare (2016): Online Abuse of Feminists as An Emerging form of Violence Against Women and Girls. The British Journal of Criminology. 30 September 2016.
https://academic.oup.com/bjc/article/doi/10.1093/bjc/azw073/2623986/Online-Abuse-of-Feminists-as-An-Emerging-form-of (link last checked on March 29, 2017)

Mapping Technology-based violence against women.

https://www.takebackthetech.net/mapit/ (link last checked on March 29, 2017)

Mapping Technology-based violence against women. Take back the tech! Top 8 findings. (2012-2014)
http://www.genderit.org/sites/default/upload/csw_map.pdf (link last checked on March 29, 2017)

MARCUM, Catherine D.; HIGGINS, George E.; RICKETTS, Melissa L. (2014): Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration. International Journal of Cyber Criminology, Vol. 8, Issue 1.

MIJATOVIĆ, Dunja (2015): Online threats of killing, rape and violence everyday reality for too many female journalists.
https://www.indexoncensorship.org/2015/08/dunja-mijatovic-online-threats-of-killing-rape-and-violence-everyday-reality-for-too-many-female-journalists/ (link last checked on March 29, 2017)

MORENO, Megan (2016): Electronic harassment: Concept map and definition.
https://www.ncjrs.gov/pdffiles1/nij/grants/249933.pdf (link last checked on March 29, 2017)

MONTAGNA, Anthony Stephen (2011): When Words Harm: Cyber Bullying: What Should the Legal Consequences Be for Abusive Speech? Is it Protected? Should it Be a Crime or Sanctioned Under Civil Liability Law? (June 9, 2011)
http://dx.doi.org/10.2139/ssrn.1861565 (link last checked on March 29, 2017)

NCJRS Special Feature: Internet Safety - Cyberbullying and Cyberstalking (with several links to granted scientific papers on this issue)
https://www.ncjrs.gov/internetsafety/cyber.html (link last checked on March 29, 2017)

NOTAR, Charles E.; PADGETT, Sharon; RODEN, Jessica (2013): Cyberbullying: A Review of the Literature. Universal Journal of Educational Research 1(1): 1-9, 2013
http://files.eric.ed.gov/fulltext/EJ1053975.pdf (link last checked on March 29, 2017)

NOTAR, CHARLES E.; PADGETT, SHARON; RODEN, JESSICA (2013): Cyberbullying: Resources for Intervention and Prevention. Universal Journal of Educational Research 1(3): 133-145, 2013.

NYST, Carly (2014): Internet intermediaries and violence against women online. Facebook: A case study. July 2014.

PAASONEN, Susanna (2010): Labors of love: netporn, Web 2.0 and the meanings of amateurism. New Media Society, 2010 12: 1297.

PACE (2016): Ending cyberdiscrimination and online hate.
https://goo.gl/gWuR9t (link last checked on March 29, 2017)

PEW RESEARCH CENTER (July 2017): "Online Harassment 2017" http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/07/10151519/PI_2017.07.11_Online-Harassment_FINAL.pdf

PLAN INTERNATIONAL, "Because I am a Girl. The State of the World's Girls 2010. Digital and Urban Frotniers: Girls in a Changing Landscape" https://www.itu.int/en/ITU-D/Digital-Inclusion/Women-and-Girls/Documents/ReportsModules/BIAAG%202010%20EN.pdf

ROGERS, Vanessa (2011): Kyberšikana (Cyberbullying). Praha: Portál, 2011. 97 p. ISBN: 978-80-7367-984-2.

STONE, Kelly (2014): Looking at bullying and cyberbullying: mapping approaches and knowledge. Study for the Scotland's Commissioner for Gender and Young People (2014).

http://www.cypcs.org.uk/ufiles/Looking-at-bullying-and-cyberbullying.pdf (link last checked on March 29, 2017)

ŠEVČÍKOVÁ, Anna (2014). Děti a dospívající online (Children and adolescents online). Praha: Grada Publishing. 183 p. ISBN: 978-80-247-5010-1.

SHORT, Donn (2013): AB v Bragg Communications: Law's Next Steps: Should Bullying be a Tort ... or Even a Crime? Manitoba Law Journal, Vol. 37, No. 1, 2013.
https://ssrn.com/abstract=2476744 (link last checked on March 29, 2017)

STAIRWAY FOUNDATION INC. "Cybersafe survey 2015"
http://www.cybersafe.asia/wp-content/uploads/2016/03/Cybersafe-Survey_LOWRES.pdf

TOKUNAGA, Robert S. (2010): Following you home from school: A critical review and synthesis of research on cyberbullying victimization. Computers in Human Behaviour, 26(3).

TSITSIKA, Artemis; JANIKIAN, Mari; WÓJCIK, Szymon; MAKARUK, Katarzyna; TZAVELA, Eleni; TZAVARA, Chara; GREYDANUS, Donald; MERRICK, Joav; RICHARDSON, Clive (2015): Cyberbullying victimization prevalence and associations with internalizing and externalizing problems among adolescents in six European countries. Computers in Human Behavior 51 (2015).

REED, Lauren A.; TOLMAN, Richard M.; WARD L. Monique (2016): Snooping and Sexting - Digital Media as a Context for Dating Aggression and Abuse Among College Students. Violence Against Women. Volume: 22 issue: 13, page(s): 1556-1576.
http://journals.sagepub.com/doi/full/10.1177/1077801216630143 (link last checked on March 29, 2017)

Stark, Evan (2007): Coercive control: How men entrap women in personal life. Oxford, UK: Oxford University Press.

Stark, Evan (2012): Looking beyond domestic violence: Policing coercive control [Special issue]. Journal of Police Crisis Negotiations, 12, 199-217

UN Broadband Commission for Digital Development Working Group on Broadband and Gender. "Cyberviolence against Women and Girls" (2015)
http://www.unwomen.org/en/digital-library/publications/2015/9/cyberviolence-against-women-and-girls (link last checked on March 29, 2017)

UN Broadband Commission Working Group on Gender. Combatting Online Violence Against Women & Girls (2015): A Worldwide Wake-up Call. September 2015
http://www.broadbandcommission.org/publications/Pages/bb-and-gender-2015.aspx (link last checked on 15 January 2018)

UNODC (2015): Study of the Effects of New Information Technologies on the Abuse and Exploitation of Children.
https://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf (link last checked on March 29, 2017)

URBAN, Jennifer Ann (2017): The Need for Strict and Defined Cyberbullying Laws (November 20, 2013). http://dx.doi.org/10.2139/ssrn.2418521 (link last checked on March 29, 2017)

VAN DOORN, Niels (2011): Digital spaces, material traces: How matter comes to matter in online performances of gender, sexuality and embodiment. Media Culture Society, Volume: 33 issue: 4, page(s): 531-547.

VAN LEEUWEN, J.C. (2012): Literature review on the research on cyberbullying definitions. Universiteit Twente.
https://fr.slideshare.net/RicovLeeuwen/jc-van-leeuwen-2012-literature-review-on-cyberbullying-definitions (link last checked on March 29, 2017)

WATTS, Lynette K.; WAGNER, Jessyca; VELASQUEZ, Benito; BEHRENS, Phyllis I. (2017): Cyberbullying in higher education: A literature review. Computers in Human Behavior, Volume 69, April 2017, Pages 268–274.

WIKIGENDER: http://www.wikigender.org/online-discussion-combatting-online-violence-against-women-and-girls/ (link last checked on March 29, 2017)

WITTES, Benjamin; POPLIN, Cody; JURECIC, Quinta & SPERA, Clara. Sextortion (2016): Cybersecurity, teenagers, and remote sexual assault. Center for Technology Innovation at Brookings. May 2016.

WOODLOCK, Delanie (2016): The Abuse of Technology in Domestic Violence and Stalking. Violence Against Women. Volume: 23 issue: 5, page(s): 584-602
http://journals.sagepub.com/doi/full/10.1177/1077801216646277 (link last checked on March 29, 2017)

5.2 Sites web

http://cookie.sk/
www.detinawebe.sk
https://goo.gl/ctBT63 (questionnaire en ligne)
http://www.nezavislost.sk
www.nobullying.com
www.ovce.sk
www.puresight.com
www.saferinternetday.org
www.zodpovedne.sk/index.php/en/
http://www.zodpovedne.sk/index.php/en/books,-manuals (à télécharger gratuitement)

5.3 Liens vers les références fournies par les Parties et les observateurs

5.3.1 Autriche

https://www.ispa.at/wissenspool/broschueren/broschueren-detailseite/broschuere/detailansicht/the-online-zoo-english.html

5.3.2 France

http://www.egalite-femmes-hommes.gouv.fr/wp-content/uploads/2017/04/GuideCyberviolences-3.pdf

http://cache.media.education.gouv.fr/file/11_-_novembre/10/2/2016_non_harcelement_guide_prevention_cyberviolence_WEB_654102.pdf

5.3.3 Italie

https://rm.coe.int/16803060a7

5.3.4 Île Maurice

http://cybersecurity.ncb.mu/English/Documents/Knowledge%20Bank/Guidelines/Guideline%20on%20Social%20Networks.pdf

http://www.ncb.mu/English/Documents/Booklet/Prefinal%20Booklet.pdf

http://mtci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf

5.3.5 Norvège

http://kriminalitetsforebygging.no/wp-content/uploads/2017/05/Kriminalitet-blant-barn-og-unge-i-Norge-2012-2016.pdf

5.4 Instruments internationaux pertinents

5.4.1 Instruments contraignants

5.4.1.1 Instruments juridiquement contraignants du Conseil de l'Europe

Convention de sauvegarde des droits de l'homme et des libertés fondamentales (telle que modifiée par le Protocole n° 11) (Rome, 4 novembre 1950) https://rm.coe.int/1680063776

Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (Istanbul, 11 mai 2011) https://rm.coe.int/1680084840

Convention du Conseil de l'Europe pour la protection des enfants contre l'exploitation et les abus sexuels (Lanzarote, 27 octobre 2007)
https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_FR.pdf

Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains (Varsovie, 16 mai 2005) https://rm.coe.int/1680083731

Charte sociale européenne (révisée) (Strasbourg, 3 mai 1996) https://rm.coe.int/168007cf94

Convention européenne relative au dédommagement des victimes d'infractions violentes (Strasbourg, 24 novembre 1983) https://rm.coe.int/1680079752

Convention sur les relations personnelles concernant les enfants (Strasbourg, 15 mai 2003)
https://rm.coe.int/0900001680083729

Convention sur la cybercriminalité (Budapest, 23 novembre 2001)
https://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/0900001680081561

5.4.1.2 Instruments juridiques des Nations Unies

Pacte international relatif aux droits civils et politiques (New York, 16 décembre 1966) https://www.ohchr.org/fr/professionalinterest/pages/ccpr.aspx

Pacte international relatif aux droits économiques, sociaux et culturels (PIDESC) (New York, 16 décembre 1966) https://www.ohchr.org/FR/ProfessionalInterest/Pages/CCPR.aspx

Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes (CEDAW) (New York, 18 décembre 1979)
https://www.ohchr.org/FR/ProfessionalInterest/Pages/CEDAW.aspx

Protocole facultatif à la Convention sur l'élimination de toutes les formes de discrimination à l'égard des femmes (New York, 6 octobre 1999)
https://www.ohchr.org/FR/ProfessionalInterest/Pages/OPCEDAW.aspx

Déclaration sur l'élimination de la violence à l'égard des femmes (*proclamée par l'Assemblée générale dans sa résolution 48/104 du 20 décembre 1993,* New York)
https://www.ohchr.org/FR/ProfessionalInterest/Pages/ViolenceAgainstWomen.aspxb

Convention relative aux droits de l'enfant (*adoptée et ouverte à la signature, à la ratification et à l'adhésion par l'Assemblée générale dans sa résolution A/44/25 du 20 novembre 1989, New York)* https://www.ohchr.org/fr/professionalinterest/pages/crc.aspx

Protocole facultatif à la Convention relative aux droits de l'enfant, concernant la vente d'enfants, la prostitution des enfants et la pornographie mettant en scène des enfants (OP- CRC-SC) (*adopté et ouvert à la signature, ratification et adhésion par la résolution A/RES/54/263 du 25 mai 2000 de l'Assemblée générale,* New York*)* https://www.ohchr.org/FR/ProfessionalInterest/Pages/OPSCCRC.aspx

Protocole facultatif à la Convention relative aux droits de l'enfant, concernant une procédure de présentation de communications (New York, 14 avril 2014) https://www.ohchr.org/FR/ProfessionalInterest/Pages/OPICCRC.aspx

Recommandation générale n° 19 sur la violence à l'égard des femmes (1992) http://hrlibrary.umn.edu/gencomm/french/WOMEN19.htm

5.4.1.3 Instruments juridiques de l'UE

Directive 97/80/CE du Conseil relative à la charge de la preuve dans les cas de discrimination fondée sur le sexe *(adoptée le 15 décembre 1997).* https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31997L0080&from=PL

Directive 2002/73/CE du Conseil relative à la mise en œuvre du principe de l'égalité de traitement entre hommes et femmes en ce qui concerne l'accès à l'emploi, à la formation et à la promotion professionnelles, et les conditions de travail (*adoptée par le Parlement européen et le Conseil le 23 septembre 2002)* https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32002L0073

Directive 2004/113/CE du Conseil relative à la mise en œuvre du principe de l'égalité de traitement entre les femmes et les hommes dans l'accès aux biens et services et la fourniture de biens et services *(adoptée le 13 décembre 2004)* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0113:FR:HTML

Décision-cadre du Conseil relative au statut des victimes dans le cadre de procédures pénales *(adoptée avant le 15 mars 2001)* https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX%3A32001F0220

Recommandation du Conseil sur la prévention des blessures et la promotion de la sécurité *(adoptée le 31 mai 2007)* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:164:0001:0002:FR:PDF

5.4.1.4 Instruments juridiques adoptés dans le cadre d'autres organisations internationales régionales (OEA, OUA)

Convention interaméricaine sur la prévention, la sanction et l'élimination de la violence contre les femmes (Belém do Pará, 9 juin 1994) https://www.oas.org/en/mesecvi/docs/BelemDoPara-FRANCAIS.pdf

Protocole à la Charte africaine des droits de l'homme et Peoples´ Droits des femmes en Afrique (Maputo, 11 juillet 2003) https://www.un.org/fr/africa/osaa/pdf/au/protocol_rights_women_africa_2003f.pdf

5.4.2 Instruments juridiques non contraignants/non contraignants

5.4.2.1 Instruments juridiquement non contraignants du Conseil de l'Europe

Recommandation Rec (2006)8 sur l'assistance aux victimes de la criminalité *(adoptée par le Comité des Ministres le 14 juin 2006 lors de la 967e réunion des Délégués Ministers´)* https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805d809f

Recommandation Rec (2005)5 sur les droits des enfants vivant en institution *(adoptée par le Comité des Ministres le 16 mars 2005 lors de la 919e réunion des Délégués Ministers´)* https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805daab2

Recommandation Rec (2002)5 sur la protection des femmes contre la violence *(adoptée par le Comité des Ministres le 30 avril 2002 lors de la 794e réunion des Délégués Ministers´)* https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805e2614

Recommandation n° R (99)19 concernant la médiation en matière pénale *(adoptée par le Comité des Ministres le 30 avril 2002 lors de la 490e réunion des Délégués)* https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168062e03b

Recommandation n° R (93)2 sur les aspects médico-sociaux de la maltraitance des enfants *(adoptée par le Comité des Ministres le 22 mars 2002 lors de la 794e réunion des Délégués Ministers´)* https://rm.coe.int/16804eebb5

Recommandation n° R(91) 9 sur les mesures d'urgence concernant la violence dans la famille *(adoptée par le Comité des Ministres le 9 septembre 1991 lors de la 461e réunion des Délégués Ministers´)* https://rm.coe.int/16804bfa85

Recommandation n° R (85) 11 sur la position de la victime dans le cadre du droit pénal et de la procédure pénale *(adoptée par le Comité des Ministres le 28 juin 1985 lors de la 387e réunion des Délégués Ministers´)* https://rm.coe.int/16804dccae

Recommandation n° R (85) 4 sur la violence dans la famille *(adoptée par le Comité des Ministres le 26 mars 1985 lors de la 382e réunion des Délégués Ministers´)* https://bice.org/app/uploads/2014/06/recommandation_R85_4_FR.pdf

5.4.2.2 Assemblée parlementaire du Conseil de l'Europe (APCE) instruments juridiquement non contraignants (résolutions et recommandations)

Résolution 1654 (2009) sur les fœmides *(adoptée par l'APCE le 30 janvier 2009)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzcxNiZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NzE2

Recommandation 1861 (2009) sur les fœmides *(adoptée par l'APCE le 30 janvier 2009)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzcxNyZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NzE3

Résolution 1635 (2008) sur la lutte contre la violence à l'égard des femmes : vers une convention du Conseil de l'Europe *(adoptée par l'APCE le 3 octobre 2009)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzY4MiZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3Njgy

Recommandation 1847 (2008) sur la lutte contre la violence à l'égard des femmes : vers une Convention du Conseil de l'Europe *(adoptée par l'APCE le 3 octobre 2009)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzY4MyZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3Njgz

Résolution 1582 (2007) « Les parlements unis pour combattre la violence domestique contre les femmes » : évaluation à mi-parcours des campagnes *(adoptée par l'APCE le 5 octobre 2007)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzU5NCZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NTk0

Recommandation 1817 (2007) sur les parlements unis dans la lutte contre la violence domestique à l'égard des femmes : évaluation à mi-parcours de la campagne *(adoptée par l'APCE le 5 octobre 2007)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzU5NiZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NTk2b

Recommandation 1777 (2007) sur les agressions sexuelles liées aux « drogues du viol » *(adoptée par l'APCE le 22 janvier 2007)*
http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzQ5OCZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NDk4

Résolution 1512 (2006) sur Les parlements unis dans la lutte contre la violence domestique envers les femmes *(adoptée par l'APCE le 28 juin 2006)*
http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzQ2NCZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NDY0

Recommandation 1723 (2005) sur les mariages forcés et les mariages d'enfants *(adoptée par l'APCE le 5 octobre 2005)*
http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0yMTA2NSZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTIxMDY1

Résolution 1327 (2003) sur les crimes dits « d'honneur » *(adoptée par l'APCE le 4 avril 2003)*
http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzEwNiZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3MTA2

Résolution 1247 (2001) sur les mutilations génitales féminines *(adoptée par la Commission permanente, agissant au nom de l'APCE le 22 mai 2001)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNjkxNCZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE2OTE0

Recommandation 1450(2000) sur la violence à l'égard des femmes en Europe *(adoptée par l'APCE le 3 avril 2000)*
http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNjc4MyZsYW5nPUZS&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE2Nzgz

5.5 Examples of domestic legislation and policies on cyberviolence

5.5.1 Andorra

Summaries or extracts of domestic legal provisions regarding cyberbullying, cyberstalking or other forms of cyberviolence.

The Principality of Andorra includes the following domestic legal provisions related to cybercrime:

- Law 20/2014, of 16 October, regulating electronic contracting and operators developing their economic activity in a digital space. https://www.bopa.ad/bopa/026065/Pagines/lo26065006.aspx

Article 9. Règim general de responsabilitat dels operadors (*General liability of servers*)
Article 39. Responsabilitat *(Liability*)

CRIMINAL CODE

- Legislative decree of 29-4-2015, publishing the revised organic Law 9/2005 of 21 February, of the Criminal Code.

https://www.bopa.ad/bopa/027038/Documents/la27038001.pdf

We mention hereinafter the main dispositions of the Criminal Code that are used by the judges to incriminate cybercrime:

Títol preliminar. Les garanties penals i l'aplicació de la llei penal (*preliminar title: criminal law principles and territorial field of application of criminal law*)
Article 8. Aplicació de la llei penal en l'espai (*territorial field of aplication of criminal law*)

Llibre primer. Part general Títol I. La infracció penal. Capítol primer. Regles generals sobre delictes i contravencions penals. (*General rules on crimes)*
Article 19. Provocació (*provocation*)

Títol III. Conseqüències accessòries del delicte referides a les persones físiques o a les persones jurídiques (*consequences of crimes aplicable to physical or legal persons*)
Article 71. Altres conseqüències (*other consequences*)

Títol VII. Delictes contra la llibertat sexual. Capítol quart. Delictes relatius a la pornografia i les conductes de provocació sexual (*crimes against sexual freedom; chapter 4 : Pornography and sexual provocation*).
Article 155. Utilització de menors i incapaços per a la pornografia (*use of minors or incapacitated persons for pornography)*
Article 156. Exhibicionisme (*exhibitionism*)
Article 157. Difusió de pornografia entre menors d'edat (*pornography diffusion amongst minors*)

Títol IX. Delictes contra l'honor (*crimes against honor)*
Article 172. Calúmnia (*calumny*)
Article 173. Difamació (*libel*)
Article 174. Injúria *(insult*)
Article 175. Concepte de publicitat (*concept of publicity*)
Article 176. Responsabilitat civil solidària (*indivisible civil liability*)
Article 177. Retractació (*retraction*)
Article 178. Publicació de la sentència (*publication of a judgement*)
Article 180. Calúmnia i difamació en judici (*calumny and libel action during a judicial procedure)*

Títol X. Delictes contra la intimitat i la inviolabilitat de domicili Capítol primer. Descobriment i revelació de secrets (*crimes against privacy and the inviolability of home; chapter I: uncovering and revealing private/Secret information*)
Article 182. Descobriment de secrets (*revealing secrets*)
Article 183. Escoltes il·legals i conductes afins (*illegal phone tapping and similar behaviours*)
Article 184. Obtenció o ús il·lícit de dades personals automatitzades (*illegal use or obtention of automatized data)*
Article 185. Qualificació per la revelació (*revelation*)
Article 186. Dades especialment protegides (*specially protected data*)
Article 209. Estafa qualificada (*qualified fraud*)
Article 210. Estafa informàtica (*informatic fraud*)
Article 225. Danys informàtics (*informatic damage*)

Títol XII. Delictes contra l'ordre socioeconòmic. Capítol segon. Delictes contra la propietat intel·lectual i industrial. Capítol tercer. Delictes relatius al mercat i als consumidors. (*crimes against the socio-economical order, chapter II: crimes against intellectual propertery, chapter III: crimes against the market and consumers)*
Article 229. Delictes contra la propietat intel·lectual (*crimes against intellectual property*)
Article 230. Delictes contra els drets de patent o models d'utilitat (*Crimes against copyright*)
Article 231. Delictes contra els drets de marc (*crimes against registered brand rights*)
Article 236. Indicacions enganyoses (*false information*)
Article 237. Engany al consumidor (*fraud to the consumer*)

Capítol quart. Delictes contra l'activitat mercantil de les empreses. (*crimes against companies activities*)
Article 241. Empresa fictícia (*fictitious companies*)
Article 243. Ús fraudulent de targeta de crèdit (*fraud on Credit card*)

Capítol setè. Delictes contra les garanties dels drets fonamentals.
Article 349. Delicte contra la inviolabilitat de la correspondència (*crime against the inviolability of correspondence*)

Títol XXIII. Delictes contra la seguretat en el tràfic jurídic. Capítol segon. Falsedat de documents, d'enregistraments tècnics i de dades informàtiques. Secció tercera. Falsedat de dades informàtiques. Capítol tercer. Falsedats personals. (*crimes against legal safety - false documents and data, registrations, false electronic data*)
Article 432. Actes preparatoris punibles (*preparatory illegal acts*)
Article 446. Creació o alteració de dades informàtiques (*creation or alteration of electronical data*)
Article 447. Ús de dades informàtiques falses o alterades (*use of false or modified electronical data*)
Article 448. Usurpació de la identitat (*identity theft*)

Llibre tercer. Contravencions penals Títol II. Contravencions penals contra el patrimoni.
Article 482. Defraudacions (*Defraudations*)

Domestic policies, strategies or responses to cyberviolence.

Andorra became the 50th member State of the Budapest Convention on Cybercrime. Andorra signed the Convention and its additional Protocol on 23 April 2013 and ratified it in Strasbourg during the international conference on 16 November 2016. This was a clear step and political sign of the political will to upgrade the legislative framework and prosecute even more cybercrime, and join the network of direct judicial cooperation that the Budapest Convention creates.
As this accession has come into force recently, on 1 March 2017, Andorra does not have yet any specific national cybercrime or cybersecurity strategy neither agency responsible for these topics.

However Andorra has had for years now the Computer-Crime Unit within the National Police Criminal Investigation Unit that assumes all cases related to cybercrime and cybersecurity. Additionally, there is the National Plan of prevention of Bullying and Harassment at School 2016-2019, where the Government of Andorra has identified and includes four typologies of harassment and its detailed instruments for prevention: physical, verbal, social exclusion and cyber harassment.
The Government of Andorra is planning nowadays to work on an inclusive cybercrime policy and strategy to fight against the increasing number of cyberviolence cases.
https://www.bopa.ad/bopa/028058/Pagines/GD20161007_09_42_06(2016-10-07_12-07-56_89855).aspx

5.5.2 Austria

Summaries or extracts of domestic legal provisions regarding cyberbullying, cyberstalking or other forms of cyberviolence.

Criminal Code

Persistent harassment involving telecommunication or computer systems § 107c.
(1) Any person who, using a telecommunication or computer system in a manner that can cause unreasonable interference with the lifestyle of the other person, continuously over a longer period of time 1. defames another in a way that can be perceived by a larger number of people, or 2. makes facts or visual material of the personal sphere of another available to a larger number of people without the consent of the other person is liable to imprisonment for up to one year or a fine not exceeding 720 penalty units.
(2) The person is liable to imprisonment for up to three years if the offence results in the suicide or a suicide attempt by the victim under para. 1.

Initiating sexual contact with persons under the age of 14 § 208a.
(1) Any person who 1. by way of telecommunication or by use of a computer system, or 2. in any other way by deceiving about his or her purpose proposes a personal meeting or agrees to such a meeting with a person under the age of 14 for the purpose of committing an offence under §§ 201 to 207a para. 1 subpara. 1 on that person and takes concrete acts of preparation to eventuate the personal meeting with that person is liable to imprisonment for up to two years.
(1a) Any person who by way of telecommunication or by use of a computer system establishes contact with a person under the age of 14 for the purpose of committing an offence under § 207a paras. 3 or 3a in relation to a pornographic image (§ 207a para. 4) of that person is liable to imprisonment for up to one year or a fine not exceeding 720 penalty units.
(2) A person is not liable under paras. 1 and 1a if the person freely and before the authorities (§ 151 para. 3) become aware of the person's culpability abandons the person's plans and informs the authorities of the person's culpability.

Domestic policies, strategies or responses to cyberviolence.

In respect of prevention, Austria would like to highlight a publication[109] from the private sector, namely ISPA - Internet Service Providers Austria (ISPA was founded in 1997 as a non-profit association which represents the interests of more than 200 members from all sectors around the Internet industry as a voluntary interest group). It's a book for children in order to make them aware at a very early stage about the risks on the Internet which is also available in English and Arabic languages.

[109] https://www.ispa.at/wissenspool/broschueren/broschueren-detailseite/broschuere/detailansicht/the-online-zoo-english.html (link checked last 11 July 2017).

5.5.3 Canada

Provision in the Criminal Code addressing cyberbullying

Publication, etc., of an intimate image without consent

Section 162.1 (1) Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty

> (a) of an indictable offence and liable to imprisonment for a term of not more than five years; or
>
> (b) of an offence punishable on summary conviction.

Definition of *intimate image*

(2) In this section, intimate image means a visual recording of a person made by any means including a photographic, film or video recording,

> (a) in which the person is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity;
>
> (b) in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and
>
> (c) in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed.

Defence

(3) No person shall be convicted of an offence under this section if the conduct that forms the subject-matter of the charge serves the public good and does not extend beyond what serves the public good.

Question of fact and law, motives

(4) For the purposes of subsection (3),

> (a) it is a question of law whether the conduct serves the public good and whether there is evidence that the conduct alleged goes beyond what serves the public good, but it is a question of fact whether the conduct does or does not extend beyond what serves the public good; and
>
> (b) the motives of an accused are irrelevant.

Depending on the nature of the activity involved, a number of Criminal Code offences may apply to instances of bullying or cyberbullying, [1] including:

- criminal harassment (section 264)
- uttering threats (section 264.1);
- intimidation (subsection 423(1)),
- mischief in relation to data (subsection 430(1.1));
- unauthorized use of computer (section 342.1);
- identity fraud (section 403);
- extortion (section 346);
- false messages, indecent or harassing telephone calls (section 372);
- counselling suicide (section 241);
- defamatory libel (sections 298-301);
- incitement of hatred (section 319); and,
- child pornography offences (section 163.1);

5.5.4 Chile

Summaries or extracts of domestic legal provisions regarding cyberbullying, cyberstalking or other forms of cyberviolence.

a) Legal provisions on school violence

Law Nr 20,536 on school violence (School Violence Law or "SVL") was enacted on September 17th, 2011 (http://bcn.cl/1uvxm), amending the General Education Act ("GEL") contained in Law Nr. 20,370 (http://bcn.cl/1uxh9). Its mail goal is to achieve good internal relations in schools (Magendzo, Toledo, Gutiérrez, "Descripción y análisis de la Ley sobre Violencia Esocal (N° 20.536): dos paradigmas antagónicos", pp. 381, 387). Under these legal provisions, internal school bodies are entrusted with the promotion of internal relations and the prevention of any form of physical or psychological violence (Art. 15 of GEL, as amended by SVL). Furthermore, school members (in a broad sense) shall report acts of physical or psychological violence, aggression or bullying affecting any student and not doing so shall be subject to fines in some cases (Art. 16 D of GEL, as amended by SVL). In addition, internal school regulations on these matters are to be in force, covering prevention policies, protocols dealing with related infringements and appropriate sanctions. This law does not impose criminal sanctions. Under said law, the definition of bullying ("acoso escolar") comprises actions or omissions whichever the means used, including those of a technological nature (Art. 16 B of GEL, as amended by SVL).

b) Other relevant legal provision

Bullying and the reaction thereto have been challenged before superior courts ("Cortes de Apelaciones") by means of claims seeking emergency remedies to wrongdoings affecting a number of fundamental rights as define in the Art. 19 *et seq.* of Constitution (see Matte, "Sanciones disciplinarias por agresiones desplegadas por alumnos a través de un fotolog. Jurisprudencia constitucional sobre bullying en Chile", passim).

c) Grooming offence

Art. 366 quáter of the Chilean Criminal Code was amended in 2011, by means of Law Nr. 20,526, in order to sanction grooming (see Matus, Ramírez, Lecciones de Derecho Penal chileno. Parte espcial, tomo I, 3rd ed., 2014, p. 346). As amended, this provision sanctions acts that could be oriented to the commission of more serious offenses (e.g. rape), albeit this particular offense takes place even if the latter purpose is not achieved or even in the absence of such purpose. In fact, this offence is committed when, the offender, for the purpose of sexually arousing himself or a third party, exposes a minor (14 years old or less) to acts of sexual nature, or to pornographic material. The aforementioned provision also contemplates the punishment of forcing minors to commit acts of sexual nature themselves in front of the offender or a third party, or the recording, delivery or display of images or recording of sexual content of themselves. The aforementioned provision is also applicable when the offences are committed from afar through means of electronic nature, as expressly stated therein. Additionally, misrepresentation of identity or age increases the severity of sanctions to be applied.

Links to domestic policies, strategies or responses to cyberviolence.

https://www.supereduc.cl/resguardo-de-derechos/no-mas-bulllying-que-debemos-saber/

http://www.internetsegura.cl/observatorio/

http://www.investigaciones.cl/jenafam/sitio_jenafam/jenafam/descargas/archivos/bullying/TRIPTICO%20BULLYNG.pdf

5.5.5 Czech Republic

Summaries or extracts of domestic legal provisions regarding cyberbullying, cyberstalking or other forms of cyberviolence.

Criminal Code

Section 145 **Grievous Bodily Harm**
(1) Whoever intentionally inflicts grievous harm to the health of another person shall be sentenced to imprisonment for three to ten years.
(2) An offender shall be sentenced to imprisonment for five to twelve years if he/she commits act referred to in Sub-section (1)
a) on two or more persons,
b) on a pregnant woman,
c) on a child under the age of fifteen years,
d) on a witness, expert or interpreter in connection with the performance of their obligations,
e) on a medical worker during performance of the medical profession or employment aimed at saving life or health, or on a person who fulfilled his/her similar obligation of saving life, health or property arising from his/her employment, profession, position or function, or imposed by law,
f) on another person for their true or presupposed race, belonging to an ethnical group, nationality, political beliefs, religion or because of his/her true or presupposed lack of religious faith,
g) repeatedly or after he/she committed another especially serious felony connected with intentional infliction of grievous bodily harm or death or its attempt, or
h) out of a condemnable motive.
(3) An offender shall be sentenced to imprisonment for eight to sixteen years, if he/she causes death by the act referred to in Sub-section (1).
(4) Preparation is criminal.

Section 146 **Bodily Harm**
(1) Whoever intentionally harms another person's health shall be sentenced to imprisonment for six months to three years.
(2) An offender shall be sentenced to imprisonment for one year to five years, if he/she commits the act referred to in Sub-section (1)
a) on a pregnant woman,
b) on a child under the age of fifteen years,
c) on a witness, expert or interpreter in connection with the performance of their obligations,
d) on a medical worker during performance of the medical profession or employment aimed at saving life or health, or on a person who fulfilled his/her similar obligation of saving life, health or property arising from his/her employment, profession, position or function, or imposed by law, or
e) on another person for their true or presupposed race, belonging to an ethnical group, nationality, political beliefs, religion or because of his/her true or presupposed lack of religious faith.
(3) An offender shall be sentenced to imprisonment for two to eight years, if he/she causes severe harm to health by the act referred to in Sub-section (1).
(4) An offender shall be sentenced to imprisonment for five to ten years, if he/she causes death by the act referred to in Sub-section (1).

Section 168 **Trafficking in Human Beings**
(1) Whoever forces, procures, hires, incites, entices, transports, conceals, detains, adopts or consigns a child to be used for
a) sexual intercourse or other forms of sexual abuse or harassment, or for production of pornographic works by another,
b) extraction of tissue, cell, or organs from his/her body by another,
c) service in the armed forces,

d) slavery or servitude, or
e) forced labour or other forms of exploitation, or
who profits on such a conduct,
shall be sentenced to imprisonment for two to ten years.
(2) The same sentence shall be imposed to anyone who forces, procures, hires, incites, entices, transports, hides, detains, adopts or consigns a person other than referred to in Sub-section (1) by using violence, threat of violence or other grievous harm or deceit, or by abusing his/her error, distress, or addiction in order to use him/her for
a) sexual intercourse or other forms of sexual abuse or harassment, or for the production of pornographic works by another,
b) extraction of tissue, cell, or organs from their body by another,
c) service in the armed forces,
d) slavery or servitude, or
e) forced labour or other forms of exploitation, or
who profits on such conduct.
(3) An offender shall be sentenced to imprisonment for five to twelve years or to confiscation of property if he/she
a) commits then act referred to in Sub-section (1) or (2) as a member of an organised group,
b) exposes another person to a risk of grievous bodily harm or death by such an act,
c) commits such an act with the intention to gain a substantial profit for him-/herself or for another, or
d) commits such an act with the intention to use another person for prostitution.
(4) An offender shall be sentenced to imprisonment for eight to fifteen years or to confiscation of property if he/she
a) causes grievous bodily harm by the act referred to in Sub-section (1) or (2),
b) commits such an act with the intention to gain extensive profit for him-/herself or for another, or
c) commits such an act in connection to an organised group operating in several states.
(5) An offender shall be sentenced to imprisonment for ten to eighteen years or to confiscation of property, if he/she causes death by the act referred to in Sub-section (1) or (2).
(6) Preparation is criminal.

Section 171 **Illegal Restraint**
(1) Whoever restrains another from enjoying personal freedom, shall be sentenced to imprisonment for up to two years.
(2) An offender shall be sentenced to imprisonment for up to three years, if he/she commits the act referred to in Sub-section (1) with the intent to facilitate another criminal offence.
(3) An offender shall be sentenced to imprisonment for two to eight years, if he/she
a) commits the act referred to in Sub-section (1) as a member of an organised group
b) commits such an act on another for his/her true or presupposed race, belonging to an ethnical group, nationality, political beliefs, religion or because of his/her true or presupposed lack of religious faith,
c) causes physical or mental suffering by such an act,
d) causes grievous bodily harm by such an act, or
e) commits such an act with the intention to gain substantial profit for him-/herself or for another.
(4) An offender shall be sentenced to imprisonment for three to ten years if he/she
a) causes death by the act referred to in Sub-section (1), or
b) commits such an act with the intent to gain extensive profit for him-/herself or for another.

Section 175 **Extortion**
(1) Whoever forces another person by violence or by a threat of violence or another serious detriment to act, omit or to suffer something, shall be sentenced to imprisonment for six months to four years, or to a pecuniary penalty.
(2) An offender shall be sentenced to imprisonment for two to eight years, if he/she
a) commits the act referred to in Sub-section (1) as a member of an organised group,

b) commits such an act with at least two persons,
c) commits such an act with a weapon,
d) causes substantial damage by such an act,
e) commits such an act on a witness, expert, or interpreter in connection to performance of their obligations, or
f) commits such an act on another for his/her true or presupposed race, belonging to an ethnical group, nationality, political beliefs, religion or because of his/her true or presupposed lack of religious faith.
(3) An offender shall be sentenced to a sentence of imprisonment for five to twelve years, if he/she
a) causes grievous bodily harm by such an act,
b) commits such an act with the intention to enable or facilitate commission of a terrorist criminal offence financing of terrorism (Section 312d) or threatening with terrorism (Section 312f), or
c) causes extensive damage by such an act.
(4) An offender shall be sentenced to imprisonment for eight to sixteen years, if he/she causes death by the act referred to in Sub-section (1).
(5) Preparation is criminal.

Section 184 **Defamation**
(1) Whoever makes a false statement about another capable of significantly threaten his/her reputation among fellow citizens, especially harm him/her in employment, disrupt his/her family relations or cause another serious detriment, shall be sentenced to imprisonment for up to one year.
(2) An offender shall be sentenced to imprisonment for up to two years or to prohibition of activity, if he/she commits the act referred to in Sub-section (1) by press, film, radio, television, publicly accessible computer network or in another similarly effective manner.

Section 185 **Rape**
(1) Whoever forces another person to have sexual intercourse by violence or by a threat of violence, or a threat of other serious detriment, or
whoever exploits the person's vulnerability for such an act,
shall be sentenced to imprisonment for six months to five years.
(2) An offender shall be sentenced to imprisonment for two to ten years, if he/she commits the act referred to in Sub-section (1)
a) by sexual intercourse or other sexual contact performed in a manner comparable with intercourse,
b) on a child, or
c) with a weapon.
(3) An offender shall be sentenced to imprisonment for five to twelve years, if he/she
a) commits the act referred to in Sub-section (1) on a child under the age of fifteen,
b) commits such an act on a person in detention, serving a prison sentence, in protective treatment, in protective detention, in protective or institutional therapy or in another place where personal freedom is restricted, or
c) causes grievous bodily harm by such an act.
(4) An offender shall be sentenced to imprisonment for ten to eighteen years, if he/she causes death by the act referred to in Sub-section (1).
(5) Preparation is criminal.

Section 187 **Sexual Abuse**
(1) Whoever performs a sexual intercourse with a child under the age of fifteen, or whoever otherwise sexually abuses a child, shall be sentenced to imprisonment for one to eight years.
(2) An offender shall be sentenced to imprisonment for two to ten years, if he/she commits the act referred to in Sub-section (1) on a child under fifteen years of age entrusted to his/her supervision, while abusing their addiction or the offender's position and, their credibility or influence derived therefrom.

(3) An offender shall be sentenced to imprisonment for five to twelve years, if he/she causes grievous bodily harm by the act referred to in Sub-section (1).
(4) An offender shall be sentenced to imprisonment for ten to eighteen years, if he/she causes death by the act referred to in Sub-section (1).
(5) Preparation is criminal.

Section 192 **Production and other Disposal with Child Pornography**
(1) Whoever handles photographic, film, computer, electronic or other pornographic works, displaying or otherwise using a child, shall be sentenced to imprisonment for up to two years.
(2) The same sentence shall be imposed to anyone, who using information or communication technologies get the access to child pornography.
(3) Whoever produces, imports, exports, transports, offers, makes publicly available, provides, puts into circulation, sells or otherwise procures photographic, film, computer, electronic or other pornographic works that display or otherwise use a child or a person, who appears to be a child or whoever profits from such pornographic works,
shall be sentenced to imprisonment for six months to three years, to prohibition of activity or to confiscation of a thing.
(4) An offender shall be sentenced to imprisonment for two to six years or to confiscation of property, if he/she commits the act referred to in Sub-section (3)
a) as a member of an organised group,
b) by press, film, radio, television, publicly accessible computer network, or in other similarly effective way, or
c) with the intention to gain substantial profit for him-/herself or for another.
(5) An offender shall be sentenced to imprisonment for three to eight years or to confiscation of property, if he/she commits the act referred to in Sub-section (3)
a) as a member of an organised group operating in more states, or
b) with the intention to gain extensive profit for him-/herself or for another.

Section 193 **Abuse of a Child for Production of Pornography**
(1) Whoever persuades, arranges, hires, allures, entices or exploits a child for production of pornographic works and profits the child's participation in such pornographic works, shall be sentenced to imprisonment for one year to five years.
(2) An offender shall be sentenced to imprisonment for two to six years, if he/she commits the act referred to in Sub-section (1)
a) as a member of an organised group, or
b) with the intention to gain substantial profit for him-/herself or for another.
(3) An offender shall be sentenced to imprisonment for three to eight years, if he/she commits the act referred to in Sub-section (1)
a) as a member of an organised group operating in several states, or
b) with the intention to gain extensive profit for him-/herself or for another.

Section 193b **Establishment of Unauthorised Contacts with a Child**
Whoever proposes a meeting to a child under fifteen years of age with the intention to commit a criminal offence referred to in Section 187 (1), Section 192, 193, Section 202 (2) or any other sexually motivated criminal offence shall be sentenced to imprisonment for up to two years.

Section 201 **Endangering a Child's Care**
(1) Whoever, even out of negligence, endangers the intellectual, emotional, or moral development of a child by
a) enticing them to an indolent or immoral life,
b) allowing them to lead an indolent or immoral life,
c) allowing them to obtain means for themselves or for others by a criminal activity or in another condemnable manner, or
d) seriously breaching his/her obligation to take care of them or another important obligation arising from parental responsibility,

shall be sentenced to imprisonment for up to two years.
(2) Whoever allows, even out of negligence, a child to play on vending machines equipped with a technical device affecting the outcome of the game and which provides the possibility of monetary winnings, shall be sentenced to imprisonment for up to one year, to a pecuniary penalty, or to prohibition of activity.
(3) An offender shall be sentenced to imprisonment for six months to five years, if he/she
a) commits the act referred to in Sub-section (1) or (2) out of a condemnable motive,
b) continues in commission of such an act for a long period of time,
c) commits such an act repeatedly, or
d) gains substantial profit for him-/herself or for another by such act.

Section 209 **Fraud**
(1) Whoever enriches him-/herself or another by inducing error in someone, by using someone's error, or by concealing material facts and thus causing damage not insignificant to property of another, shall be sentenced to imprisonment for up to two years, to prohibition of activity, or to confiscation of a thing.
(2) An offender shall be sentenced to imprisonment for six months to three years, if he/she commits the act referred to in Sub-section (1) and has been convicted or sentenced for such an act in the past three years.
(3) An offender shall be sentenced to imprisonment for one to five years or to a pecuniary penalty, if he/she causes larger damage by the act referred to in Sub-section (1).
(4) An offender shall be sentenced to imprisonment for two to eight years, if he/she
a) commits the act referred to in Sub-section (1) as a member of an organised group,
b) commits such an act as a person having a particular obligation to defend the interests of the aggrieved person,
c) committed such an act in a state of national emergency or a state of war, natural disaster or during another event seriously threatening the life or health of people, public order or property, or
d) causes substantial damage by such an act.
(5) An offender shall be sentenced to imprisonment for five to ten years, if he/she
a) causes extensive damage by the act referred to in Sub-section (1), or
b) commits such an act in order to facilitate or enable commission of a terrorist criminal offence, financing of terrorism (Section 312d) or threatening with terrorism (Section 312f).
(6) Preparation is criminal.

Section 353 **Dangerous Threatening**
(1) Whoever threatens another with death, grievous bodily harm another serious detriment in such a way that it can raise a reasonable fear, shall be sentenced to imprisonment for up to one year or to prohibition of activity.
(2) An offender shall be sentenced to imprisonment for up to three years or to prohibition of activity, if he/she commits the act referred to in Sub-section (1)
a) as a member of an organised group,
b) against a child or a pregnant woman,
c) with a weapon,
d) on a witness, expert or interpreter in connection to performance of their duties, or
e) on a medical worker in performance of medical occupation or a profession aimed at saving lives or protection of health or on another person who was fulfilling his/her similar duty in protection of lives, health or property arising from his/her occupation, profession, position or function or imposed to him/her according to law.

Section 354 **Dangerous Pursuing**
(1) Whoever pursues another in long term by
a) threatening with bodily harm or another detriment to him/her or to persons close to him/her,
b) seeks his/her personal presence or follows him/her,
c) persistently contacts him/her by the means of electronic communications, in writing or in another way,

d) restricting him/her in his/her usual way of life, or
e) abuses his/her personal data for the purpose of gaining personal or other contact,
and this conduct is capable of raising reasonable fear for his/her life or health or lives or health of persons close to him/her, shall be sentenced to imprisonment for up to one year or to prohibition of activity.
(2) An offender shall be sentenced to imprisonment for six months to three years, if he/she commits the act referred to in Sub-section (1)
a) against a child or a pregnant woman,
b) with a weapon, or
c) with at least two persons.

5.5.6 Estonia

Recommendations by the Estonian Police
https://www.politsei.ee/et/nouanded/noorele/kuberkiusamine/
https://www.politsei.ee/et/nouanded/it-kuriteod/identiteedivargus/
https://www.politsei.ee/et/nouanded/noorele/seksuaalkuriteod-virtuaalmaailmas/

Safer Internet Centre in Estonia recommendations
http://noor.targaltinternetis.ee/kuber-kiusamine/

Safer Internet Centre in Estonia Annual report
http://www.targaltinternetis.ee/wp-content/uploads/2015/12/D1.4.2Final_public_report_eng1.pdf

Estonia.ee information materials
https://www.eesti.ee/eng/perekond/lapsed_perekonnas/laste_kaitsmine

Some news on cyber violence
http://news.err.ee/101618/children-experience-worst-cyber-bullying-in-eu
http://news.postimees.ee/3579475/hope-you-get-raped

ESTONIAN STUDENTS' PERCEPTION AND DEFINITION OF CYBERBULLYING
http://www.eap.ee/public/trames_pdf/2012/issue_4/trames-2012-4-323-343.pdf
http://eha.ut.ee/wp-content/uploads/2015/10/5_07_naruskov_luik_summary.pdf

Other Studies
http://www.targaltinternetis.ee/wp-content/uploads/2015/12/kuberkiusamine_mag_too_k_kuusk.pdf
http://www.cs.tlu.ee/instituut/opilaste_tood/bakalaureuse_ja_diplomitood/2008_kevad/Helle_Isakannu/Helle_Isakannu_Bakalaureuse_Too.pdf

EU Kids Online survey
http://www.lse.ac.uk/media@lse/research/eukidsonline/eu%20kids%20i%20(2006-9)/eu%20kids%20online%20i%20reports/eukidsonlinefinalreport.pdf
https://lsedesignunit.com/EUKidsOnline/
http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx
http://www.lse.ac.uk/media@lse/research/EUKidsOnline/ParticipatingCountries/estonia.aspx
http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsExecSummary/EstoniaExecSum.pdf

5.5.7 France

The *5e plan interministériel de mobilisation et de lutte contre toutes les violences faites aux femmes*[110] issued in April 2017 the *Guide d'information et de lutte contre les cyberviolences à caractère sexiste*[111] which contains reference to the offences and applicable sanctions for all the crimes related with hate, discrimination and violence.

Other useful links are the following:

http://www.haut-conseil-egalite.gouv.fr/

https://www.centre-hubertine-auclert.fr/sites/default/files/fichiers/actes-251114-cybersexisme-web_0.pdf

https://www.centre-hubertine-auclert.fr/sites/default/files/fichiers/cybersexisme-brochure-encadrant-e-s-s.pdf

La législation française repressive relative à ces phénomènes se trouve dans le Code Pénal :

Livre II : Des crimes et délits contre les personnes

- **Titre II : Des atteintes à la personne humaine**
  - **Chapitre II : Des atteintes à l'intégrité physique ou psychique de la personne**
    - Section 3 bis : du harcèlement moral

Article 222-33-2
Modifié par LOI n°2014-873 du 4 août 2014 - art. 40

Le fait de harceler autrui par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation des conditions de travail susceptible de porter atteinte à ses droits et à sa dignité, d'altérer sa santé physique ou mentale ou de compromettre son avenir professionnel, est puni de deux ans d'emprisonnement et de 30 000 € d'amende.

Article 222-33-2-1
Modifié par LOI n°2014-873 du 4 août 2014 - art. 40

Le fait de harceler son conjoint, son partenaire lié par un pacte civil de solidarité ou son concubin par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale est puni de trois ans d'emprisonnement et de 45 000 € d'amende lorsque ces faits ont causé une incapacité totale de travail inférieure ou égale à huit jours ou n'ont entraîné aucune incapacité de travail et de cinq ans d'emprisonnement et de 75 000 € d'amende lorsqu'ils ont causé une incapacité totale de travail supérieure à huit jours.

Les mêmes peines sont encourues lorsque cette infraction est commise par un ancien conjoint ou un ancien concubin de la victime, ou un ancien partenaire lié à cette dernière par un pacte civil de solidarité.

Article 222-33-2-2
Créé par LOI n°2014-873 du 4 août 2014 - art. 41

110 http://www.egalite-femmes-hommes.gouv.fr/5eme-plan-de-mobilisation-et-de-lutte-contre-toutes-les-violences-faites-aux-femmes-2017-2019/ (link verified last 17 July 2017).
111 http://www.egalite-femmes-hommes.gouv.fr/wp-content/uploads/2017/04/GuideCyberviolences-3.pdf (link verified last 17 July 2017)

Le fait de harceler une personne par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale est puni d'un an d'emprisonnement et de 15 000 € d'amende lorsque ces faits ont causé une incapacité totale de travail inférieure ou égale à huit jours ou n'ont entraîné aucune incapacité de travail.

Les faits mentionnés au premier alinéa sont punis de deux ans d'emprisonnement et de 30 000 € d'amende :

1° Lorsqu'ils ont causé une incapacité totale de travail supérieure à huit jours ;

2° Lorsqu'ils ont été commis sur un mineur de quinze ans ;

3° Lorsqu'ils ont été commis sur une personne dont la particulière vulnérabilité, due à son âge, à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse, est apparente ou connue de leur auteur ;

4° Lorsqu'ils ont été commis par l'utilisation d'un service de communication au public en ligne.

Les faits mentionnés au premier alinéa sont punis de trois ans d'emprisonnement et de 45 000 € d'amende lorsqu'ils sont commis dans deux des circonstances mentionnées aux 1° à 4°.

- Section 6 : de la provocation au suicide

Article 223-13
Modifié par LOI n°2009-1437 du 24 novembre 2009 - art. 50

Le fait de provoquer au suicide d'autrui est puni de trois ans d'emprisonnement et de 45 000 euros d'amende lorsque la provocation a été suivie du suicide ou d'une tentative de suicide.

Les peines sont portées à cinq ans d'emprisonnement et à 75 000 euros d'amende lorsque la victime de l'infraction définie à l'alinéa précédent est un mineur de quinze ans.

Les personnes physiques ou morales coupables du délit prévu à la présente section encourent également la peine complémentaire suivante : interdiction de l'activité de prestataire de formation professionnelle continue au sens de l'article L. 6313-1 du code du travail pour une durée de cinq ans.

Article 223-14
Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002

La propagande ou la publicité, quel qu'en soit le mode, en faveur de produits, d'objets ou de méthodes préconisés comme moyens de se donner la mort est punie de trois ans d'emprisonnement et de 45 000 euros d'amende.

Article 223-15

Lorsque les délits prévus par les articles 223-13 et 223-14 sont commis par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

Article 223-15-1
Modifié par LOI n°2009-526 du 12 mai 2009 - art. 124

Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section encourent, outre l'amende suivant les modalités prévues par l'article 131-38 :

1° (Abrogé) ;

2° Les peines mentionnées aux 2° à 9° de l'article 131-39 ;

3° La peine mentionnée au 1° de l'article 131-39 pour l'infraction prévue au deuxième alinéa de l'article 223-13.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise.

Livre II : Des crimes et délits contre les personnes

- **Titre II : Des atteintes à la personne humaine**
  - **Chapitre VI : Des atteintes à la personnalité**

Section 1 : De l'atteinte à la vie privée

Article 226-1
Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002

Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.

Article 226-2

Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1.

Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

Article 226-2-1
Créé par LOI n°2016-1321 du 7 octobre 2016 - art. 67

Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende.

Est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1.

Article 226-3
Modifié par LOI n°2016-731 du 3 juin 2016 - art. 5

Est puni de cinq ans d'emprisonnement et de 300 000 € d'amende :

1° La fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques de nature à permettre la réalisation d'opérations pouvant constituer l'infraction prévue par le second alinéa de l'article 226-15 ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 et 706-102-2 du code de procédure pénale et L. 853-2 du code de la sécurité intérieure et figurant sur une liste dressée dans des conditions fixées par décret en Conseil d'Etat, lorsque ces faits sont commis, y compris par négligence, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par ce même décret ou sans respecter les conditions fixées par cette autorisation ;

2° Le fait de réaliser une publicité en faveur d'un appareil ou d'un dispositif technique susceptible de permettre la réalisation des infractions prévues par l'article 226-1 et le second alinéa de l'article 226-15 lorsque cette publicité constitue une incitation à commettre cette infraction ou ayant pour objet la captation de données informatiques prévue aux articles 706-102-1 et 706-102-2 du code de procédure pénale et L. 853-2 du code de la sécurité intérieure lorsque cette publicité constitue une incitation à en faire un usage frauduleux.

Article 226-4
Modifié par LOI n°2015-714 du 24 juin 2015 - art. unique

L'introduction dans le domicile d'autrui à l'aide de manoeuvres, menaces, voies de fait ou contrainte, hors les cas où la loi le permet, est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

Le maintien dans le domicile d'autrui à la suite de l'introduction mentionnée au premier alinéa, hors les cas où la loi le permet, est puni des mêmes peines.

Article 226-4-1
Créé par LOI n°2011-267 du 14 mars 2011 - art. 2

Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende.

Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.

Article 226-4-2
Créé par LOI n°2014-366 du 24 mars 2014 - art. 26
Le fait de forcer un tiers à quitter le lieu qu'il habite sans avoir obtenu le concours de l'Etat dans les conditions prévues à l'article L. 153-1 du code des procédures civiles d'exécution, à l'aide de manœuvres, menaces, voies de fait ou contraintes, est puni de trois ans d'emprisonnement et de 30 000 € d'amende.
Article 226-5

La tentative des infractions prévues par la présente section est punie des mêmes peines.

Article 226-6
Modifié par LOI n°2016-1321 du 7 octobre 2016 - art. 67

Dans les cas prévus par les articles 226-1 à 226-2-1, l'action publique ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

Article 226-7
Modifié par LOI n°2009-526 du 12 mai 2009 - art. 124

Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section encourent, outre l'amende suivant les modalités prévues par l'article 131-38 :

1° (Abrogé) ;

2° L'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement l'activité professionnelle ou sociale dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ;

3° L'affichage ou la diffusion de la décision prononcée, dans les conditions prévues par l'article 131-35.

Livre II : Des crimes et délits contre les personnes

- **Titre II : Des atteintes à la personne humaine**
  - **Chapitre VII : Des atteintes aux mineurs et à la famille**

- Section 5 : De la mise en péril des mineurs :

Article 227-22
- Modifié par LOI n°2013-711 du 5 août 2013 - art. 5

Le fait de favoriser ou de tenter de favoriser la corruption d'un mineur est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Ces peines sont portées à sept ans d'emprisonnement et 100 000 euros d'amende lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communications électroniques ou que les faits sont commis dans les établissements d'enseignement ou d'éducation ou dans les locaux de l'administration, ainsi que, lors des entrées ou sorties des élèves ou du public ou dans un temps très voisin de celles-ci, aux abords de ces établissements ou locaux.

Les mêmes peines sont notamment applicables au fait, commis par un majeur, d'organiser des réunions comportant des exhibitions ou des relations sexuelles auxquelles un mineur assiste ou participe ou d'assister en connaissance de cause à de telles réunions.

Les peines sont portées à dix ans d'emprisonnement et 1 000 000 euros d'amende lorsque les faits ont été commis en bande organisée ou à l'encontre d'un mineur de quinze ans.

Article 227-22-1
- Créé par Loi n°2007-297 du 5 mars 2007 - art. 35 JORF 7 mars 2007
- Créé par Loi n°2007-297 du 5 mars 2007 - art. 35

Le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

Ces peines sont portées à cinq ans d'emprisonnement et 75 000 euros d'amende lorsque les propositions ont été suivies d'une rencontre.

Article 227-23

- Modifié par LOI n°2013-711 du 5 août 2013 - art. 5

Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque l'image ou la représentation concerne un mineur de quinze ans, ces faits sont punis même s'ils n'ont pas été commis en vue de la diffusion de cette image ou représentation.

Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.

Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques.

Le fait de consulter habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition une telle image ou représentation, d'acquérir ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30 000 euros d'amende.

Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500 000 euros d'amende lorsqu'elles sont commises en bande organisée.

La tentative des délits prévus au présent article est punie des mêmes peines.

Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image.

Article 227-24
- Modifié par LOI n°2014-1353 du 13 novembre 2014 - art. 7

Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent, incitant au terrorisme, pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75 000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur.

Lorsque les infractions prévues au présent article sont soumises par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

Article 227-26
- Modifié par LOI n°2011-525 du 17 mai 2011 - art. 150

L'infraction définie à l'article 227-25 est punie de dix ans d'emprisonnement et de 150 000 euros d'amende :

1° Lorsqu'elle est commise par un ascendant ou par toute autre personne ayant sur la victime une autorité de droit ou de fait ;

2° Lorsqu'elle est commise par une personne qui abuse de l'autorité que lui confèrent ses fonctions ;

3° Lorsqu'elle est commise par plusieurs personnes agissant en qualité d'auteur ou de complice ;

4° Lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de communication électronique ;

5° Lorsqu'elle est commise par une personne agissant en état d'ivresse manifeste ou sous l'emprise manifeste de produits stupéfiants.

5.5.8 Finland

Parties were asked to share information regarding online violence/cyberviolence by 15 July.

Unfortunately at least at this stage there is not much to share. This phenomenon as such is a new one in Finland and inquiries to the law enforcement and to the prosecution services didn't produce presentable cases (question 1). Some online offences have been a topic of a public discussion but there are no domestic policies, strategies or other specific responses focusing on this issue (question 3).

We don't have specific provisions regarding online offences/cyberbullying offences either (question 2). The coverage of these offences is unclear but nevertheless it's possible to say that acts like these are covered by many Criminal Code provisions. At least following offences are relevant in this context (offences may be committed also online):

- distribution of a sexually offensive picture and aggravated distribution of a sexually offensive picture depicting a child (Chapter 17, Sections 18 and 18(a)),
- sexual abuse of a child, aggravated sexual abuse of a child, purchase of sexual services from a young person, solicitation of a child for sexual purposes and following a sexually offensive performance of a child (Chapter 20, Sections 6, 7, 8(a), 8(b) and 8(c)),
- assault (Chapter 21, Section 5; may injure also the mental health of another),
- harassing communications, dissemination of information violating personal privacy, aggravated dissemination of information violating personal privacy, defamation and aggravated defamation (Chapter 24, Sections 1(a), 8, 8(a), 9 and 10),
- stalking (Chapter 25, Section 7(a)) and
- extortion and aggravated extortion (Chapter 31, Sections 3 and 4).

The English language translation of the Criminal Code is available on the following website:

http://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf

5.5.9 Germany

General remarks

Germany considers it **important to prevent cyberbullying and online violence**. Especially in serious cases, this may also include criminal sanctions in regard to certain forms of conduct. However, the phenomena of cyberbullying and online violence **cannot be addressed by criminal law alone**, but also require preventive measures and the raise of awareness in society.

Cyberbullying and online violence are characterized by making use of the internet and connected devices. However, the relevant conduct in the area of criminal law is **often covered by broader offences** that do not require using such devices (e.g. insult, threat or coercion). In these cases, computer devices are mainly used as an *instrument* to commit traditional offences. This is a well-known development in regard to many traditional offences due to continued digitization in all areas of society.

At least in some cases the conduct in the area of cyberbullying and online violence can also be linked to **cybercrime in a narrower sense**, involving an infringement of computer devices (e.g. hacking a computer to obtain pictures that are subsequently used for blackmailing). But even in these cases the involved cybercrime offences typically seem to be of a rather *instrumental nature*, allowing the commission of other and often more severe crimes.

As a conclusion, cyberbullying and online violence seem to involve *cybercrime in a narrower sense* only to a limited extent. Therefore the most relevant criminal offences in national legislation are **usually not directly linked to the Budapest Convention**. In this regard, it should be noted that in our view it is exactly the strength of the Convention to provide a clear focus on cybercrime in a narrower sense. While this does not exclude to analyse phenomena that are connected with cybercrime, it should be also taken care that the focus of the Convention is not blurred.

Summaries or extracts of domestic legal provisions regarding cyberbullying, cyberstalking or other forms of online violence.

Overview

As it was mentioned before, **many areas of law** are relevant for the prevention of cyberbullying and cyberviolence. Apart from criminal law (see below), corresponding provisions and rules can be found in civil law (e.g. compensation, removal and injunction), labour law (e.g. warning notice) and administrative law including police law and regulations for service providers (see below). A provision that can be mentioned in particular is section 1 of the Law for the civil law prevention of

acts of violence and stalking (*Gewaltschutzgesetz*)[112] which allows the court to take the necessary measures to prevent further conduct.

Criminal Law Provisions

Relevant **criminal law provisions** in Germany can be, for example, section 238 (Stalking), section 240 (Using threats or force to cause a person to do, suffer or omit an act), section 241 (Threatening the commission of a felony), section 176 (Child abuse), section 185 (Insult), section 186 (Defamation), section 187 (Intentional defamation), section 201 (Violation of the privacy of the spoken word) and section 201a (Violation of intimate privacy by taking photographs) of the German Criminal Code (*Strafgesetzbuch*)[113] as well as section 33 of the Law concerning copyright related to works of visual arts and photography (*Kunsturhebergesetz*).

Section 238 (Stalking) can be mentioned in particular, as it expressively includes conduct by means of telecommunications (para. 1 no. 2) or by using personal data of a person (para. 1 no. 3). The same is true for section 176 (Child abuse) which also expressly covers conduct by means of telecommunications (para. 4 no. 3 and 4).

Regulations for Service Providers

With the recent adoption of the Act to Improve Enforcement of the Law in Social Networks, Germany has introduced compliance obligations for social networks. In particular, social networks are required to remove content that is unlawful under certain provisions of the German Criminal Code within a specific time frame after having been notified about the content. This obligation exists with regard to content fulfilling e.g. section 130 (incitement to hatred), section 241 (threatening the commission of a felony), section 185 (insult), section 186 (defamation), section 187 (intentional defamation), and section 201a (violation of intimate privacy by taking photographs) of the Criminal Code. In connection with this, the act also provides for the possibility to fine social networks up to 50 million Euros for demonstrated systemic shortcomings with fulfilling the compliance obligations. The act therefore contributes to a healthier environment in social networks and thus helps to contain cyberbullying and cyberviolence. The act shall enter into force on October 1st 2017.

The act also amends section 14 para. 3 to 5 of the German Telemedia Act (*Telemediengesetz*) and provides host providers (such as social networks) with the permission from a data protection perspective to disclose personal data (data relevant for establishing the contractual relationship between user and service provider and usage data) to individuals for the purposes of enforcing civil law claims related to the content mentioned above. The legal grounds for these disclosure requests by individuals, however, are to be found in other relevant legislation, in particular the German Civil Code.

Links to domestic policies, strategies or responses to cyberviolence.

Preventing cyberbullying and cyberviolence is an important issue for the German government. Apart from legislative measures, the German government supports initiatives in this area. In 2016 the 2nd Cybermobbing Congress has been hosted under the auspices of the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth. Besides, the private association "Alliance against Cybermobbing" is a partner of the "Coalition for Digital Security" of the initiative "Deutschland sicher im Netz" under the auspices of the Federal Ministry of Interior.

[112] Available online (only in German language): http://www.gesetze-im-internet.de/gewschg/index.html
[113] Available online (in German and English language): http://www.gesetze-im-internet.de/stgb/index.html (Please note that the English version does not always reflect the latest legislation, as is, e.g., the case for section 176, 201a and 238.)

5.5.10 Israel

Summaries or extracts of domestic legal provisions regarding cyberbullying, cyberstalking or other forms of cyberviolence.

Firstly, it will be noted that the Israeli legal provisions, and in particular the Israeli Criminal Code of 1977, all apply to the internet as is. That means that criminal proceedings may be taken regarding all the offences that appear on the Israeli Criminal Code if occurred online, and when appropriate. It will be noted that alongside the Criminal Code of 1977, additional laws include criminal offences that may be used in criminal proceedings, if necessary. Such is the case regarding the Israeli Computers Act (1995), the Israeli Protection of Privacy Act (1982) or the Prevention of Sexual Harassment Act (1998).

On the matter of cyberbullying it will be noted that the Israeli legal system does not include for now a specific prohibition regarding this conduct. The conduct of "cyberbullying" may be covered by different legal provisions, based on the facts of the specific case. These provisions may include the following:

1) Article 30 to the Israeli Communications Act of 1982 forbids the use of a "Bezeq facility" to perform an act of harassment. A "Bezeq facility" is any facility or device that is used in order to transmit, receive or transfer signs, signals, visual forms, writings, voices or information using wire, wireless, an optic system or other electromagnetic systems.
   The term "Harassment" in this context was interpreted by the Israeli Supreme Court as a term that holds two different meanings, each is relevant on its own to establish the offence. The first meaning is the "technical" use of the "Bezeq facility" in order to harass. For example, calling a person numerous times on his telephone in inconvenient times. The second meaning is the "substantive" meaning, which includes using the "Bezeq facility" to convey harassing content to the victim.[114]
   As you can see, this offence, however not dedicated to tackle Cyberbullying specifically, may in fact be used to indict criminals that use "Bezeq facilities" (including, of course, e-mails, social networks, online chat rooms and so on) to harass their victims.

2) Article 3(a)(5a) to the Israeli Prevention of Sexual Harassment Act (1998) states that a sexual harassment may also be "a publication of a picture, a video or a recording of a person, focused on that person's sexuality, when the publication may humiliate or degrade that person, and when that person did not give his consent to the publication". The punishment on this conduct is five years imprisonment and the perpetrator is regarded as a sex offender after convicted.
   This Article was enacted mainly in order to tackle the phenomenon known as "revenge porn". Usually the phenomenon includes the documentation of a sexual act that was performed with consent, and then one of the people involved in the act publishes that content without the consent of the second person. This "revenge porn" is regarded as a sort of cyberviolence towards the victim, and thus may be regarded as a type of "cyberbullying".

3) Article 2 to the Israeli Protection of Privacy Act (1982) states a list of twelve conducts that may consist as an intrusion of privacy. Among other conducts, the Article states that an intrusion of privacy may be the documentation of a person when he is in his private domain; the publication of a picture of a person when the publication may humiliate or degrade that person; copying the content of a person's correspondence; or the publication of a matter regarding a person's private life, including his sexual conduct or his health condition. The intrusion of privacy in these manners is punishable by five years' imprisonment.

[114] Criminal Appeal 10462/03 Harar vs. the State of Israel (30.6.2005).

The intrusion of privacy is not a "classic" form of "cyberbullying" but nonetheless we believe that these offences help "cover" different forms of cyber-bulling conducted online.

4) Article 192 to the Israeli Criminal Code (1977) states as an offence the act of threatening another person. The Article states as an offence "threatening a person in any way in causing illegal harm to his or a different person's body, freedom, assets, reputation or livelihood, intending to frighten the person or tease him – is punishable by three years' imprisonment".
This provision is well applicable to the online environment and is often used in cases regarding intimidation or threats conducted online. In cases of "cyberbullying" this provision is often used when the perpetrator used any sort of threat in causing harm to the victim.

5) Article 144D2(a) to the Israeli Criminal Code (1977) forbids the act of incitement for violence. The Article states that "publishing a call for an act of violence, or praising or encouraging an act of violence, supporting it or expressing solidarity with it, and when based on the content of the publication and its circumstances there is a real possibility that the publication will lead to an act of violence – is punishable by five years' imprisonment".
This Article may be used to indict perpetrators that call on the infliction of violence against another person, especially in cases where the call may lead to an actual infliction of violence against the victim. "Cyberbullying" often occurs when the bullying is inflicted by the hands of a lot of different people online, simultaneously. This Article enables the prosecution to indict people who organize and encourage to infliction of violence against the victim, even in cases where the violence did not occur physically.

6) Article 4 to the Israeli Prevention of Threatening Harassment (2001) gives the Israeli court the authority to issue a warrant that forbids the harassment of the victim. This is a civil warrant and a civil proceeding, but it is noted here as a different course of action that the victim may choose.
This warrant may include the following provisions: the prohibition of spying on the victim; the prohibition of contacting the victim in any way; the prohibition of being near the victim's home or workplace and the prohibition of carrying a weapon. This course of action is a useful method of tackling harassers and is a supplementary channel to the criminal proceedings.

In addition to all these provisions, it should be noted that on August 2015 the Israeli Minister of Justice has appointed former Supreme Justice Edna Arbel to lead a committee named "a committee to form means of protecting the public and civil servants from harmful publication and bulling on the internet". The committee's members are from the public service, the academy, and the private sector, and the committee is focused on finding legal and non-legal solutions to the problem of cyberviolence and cyberbullying.

5.5.11 Italy

Summaries or extracts of domestic legal provisions regarding cyberbullying, cyberstalking or other forms of cyberviolence.

Last 17th of May 2017 the Italian Parliament has approved unanimously a long-awaited legislation to address cyberbullying. This law no. 71/2017, entitled "Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying", passed after some tragic cases of cyberbullying and violence against women in which victims have committed suicide[115].

Article 1 of the law provides a specific legal definition of cyberbullying for the first time in Italy, defining it as "whatever form of psychological pressure, aggression, harassment, blackmail, injury, insult, denigration, defamation, identity theft, alteration, illicit acquisition, manipulation, unlawful

[115] For example the Carolina Picchio and the Tiziana Cantone cases.

processing of personal data of minors and/or dissemination made through electronic means, including the distribution of online content depicting also one or more components of the minor's family whose intentional and predominant purpose is to isolate a minor or a group of minors by putting into effect a serious abuse, a malicious attack or a widespread and organized ridicule."

The law provides a strong empowerment of minors stating at Article 2 that underage victims that are at least 14 years old or their parents can now contact directly the data controller or the website or social media provider in order to present a request for blocking, remove or taking down every other personal data of the victim, after that the original data have been preserved. The request must expressly include the URLs where the content is reachable. The recipient of the request must reply after 24 hours that he takes the obligation of blocking, removing or taking down the content and after 48 hours from the request the obligation must be fulfilled.

In case the request is not fulfilled or it is impossible to determine the owner of the website or of the social media, it is possible to lodge a circumstantial claim or a report to the Italian Data Protection Authority that will proceed in the following 48 hours according to articles 143 (Handling a Claim) and 144(Reports) of the Italian Data Protection Code.

An important role is given to the prevention at school to counter cyberbullying. According to the Article 3 of the law, the Italian Ministry of Education and University will be the leader of an institutional forum composed by experts and interested stakeholders for discussing the issue of fighting cyberbullying and monitoring the effective implementation and enforcement of the law. The aim of this forum is to develop a comprehensive plan to combat and prevent cyberbullying with different initiatives like, for example, the drafting of a code of conduct for service and network providers and informative events for parents and teachers.

Finally, every school must designate a teacher for coordinating all the initiative to counter cyberbullying, with the help of the Italian Postal and Communication Police. Part of this initiative must be focused on educating the students about good and lawful online behavior, including rights and duties of online users.

Another important law that worth to be mentioned, besides the general offences concerning violence, is the specific offence for stalking included in Section 612-bis of Italian Criminal Code.

This offence, entitled "Persecutory Conducts" punishes with deprivation of liberty between 6 months and 4 years whoever, with repeated acts, threatens or harasses someone causing to the victim a persistent and serious state of anxiety or fear or causing a well-founded worry for his safety or for a safety of a close relative or, finally, forcing the victim to change his life habits.

Links to domestic policies, strategies or responses to online violence.

https://rm.coe.int/16803060a7
http://www.generazioniconnesse.it/site/it/home-page/
http://www.noisiamopari.it/site/it/home-page/
http://www.casapediatrica.it/centro-multidisciplinare-sul-disagio-adolescenziale/
http://www.bullismoedoping.it/index.php

5.5.12 Japan

Summaries or extracts of domestic legal provisions regarding cyberbullying, cyberstalking or other forms of cyberviolence.

The Anti-Stalking Act

Article 1（Purpose)
The purpose of this Act is to prevent harm against a body and the freedom and reputation of an individual, in addition, to contribute to the safety and tranquility of citizens' lives by imposing necessary restriction including provisions for punishment against stalking and defining measures of aid for victims.

Article 2（Definitions）
1. The term "Following, etc." as used in this Act means taking any of the matters listed below against a person, his/her spouse, lineal blood relatives or relatives living together or any person who has a close relationship in social life with him/her for the purpose of satisfying one's affection, including romantic feelings, toward any person or fulfilling a grudge when the said affection is unrequited.
(5) Making silent calls, or calling, transmitting using a fax machine or sending text messages through any text messaging service persistently despite his/her rejections.

2. "Sending text messages through any text messaging service" stipulated in (5) shall take any form of the following actions.
a. Making transmissions via telecommunications used to transmit information after specifying the victim as a recipient of the transmission, be it a text message, or any other kind of transmission.
b. In addition to what is stipulated in "a", ancillary to allowing a third party to view the information entered by the specific individual using telecommunications, using the relevant functions that provide the means to transmit information to the relevant individual by a third party.

3. The term "Stalking" as used in this Act shall mean repeating the Following, etc. (Matters listed in items (1) to (4) and (5) (limited to sending text messages through any text messaging service) shall only apply to actions taken in such a way as to cause feelings of anxiety or fear for his/her physical safety, tranquility of the Domicile, etc. or reputation would be harmed, or freedom of action would be significantly curtailed.)

Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child Pornography, and the Protection of Children Article7(6)

Any person who provides child pornography to unspecified persons or a number of persons or displays it in public shall be sentenced to imprisonment for not more than 5 years and/or a fine of not more than 5,000,000 yen. The same shall apply to any person who provides electromagnetic records or any other record which depicts the pose of a child, which falls under any of the categories of paragraph 3 of Article 2, to unspecified persons or a number of persons in a visible way through telecommunication lines.

Intimidation: Penal Code Article 222(1)
A person who intimidates another through a threat to another's life, body, freedom, reputation or property shall be punished by imprisonment for not more than 2 years or a fine of not more than 300,000 yen.

Compulsion: Penal Code Article 223(1)
A person who, by intimidating another through a threat to another's life, body, freedom, reputation or property or by use of assault, causes the other to perform an act which the other

person has no obligation to perform, or hinders the other from exercising his or her rights, shall be punished by imprisonment for not more than 3 years.

Defamation: Penal Code Article 230(1)
A person who defames another by alleging facts in public shall, regardless of whether such facts are true or false, be punished by imprisonment with or without work for not more than 3 years or a fine of not more than 500,000 yen.

Insults: Penal Code Article 231
A person who insults another in public, even if it does not allege facts, shall be punished by misdemeanor imprisonment without work or a petty fine.

Obstruction of Business: Penal Code Article 233
A person who damages the credit or obstructs the business of another by spreading false rumors or by the use of fraudulent means shall be punished by imprisonment for not more than 3 years or a fine of not more than 500,000 yen.

Forcible Obstruction of Business: Penal Code Article 234
A person who obstructs the business of another by force shall be dealt with in the same manner as prescribed under the preceding Article.

Display of Obscene Recording Media Containing Electromagnetic Records: Penal Code Article 175 (1)
A person who distributes or displays in public an obscene document, drawing, recording media containing such electromagnetic records or other objects shall be punished by imprisonment for not more than 2 years, a fine of not more than 2,500,000 yen or a petty fine, or both imprisonment and a fine. The same shall apply to anyone who distributes an obscene electromagnetic record or any other record by transmission of telecommunication.

Act on Prevention of Damage Caused by Provision of Private Sexual Image Records Article 3(1)
A person who provides unspecified persons or a number of persons with private sexual image records through telecommunication lines in such a way that third parties can specify the individual in that image shall be punished by imprisonment for not more than 3 years or a fine of not more than 500,000 yen.

Links to domestic policies, strategies or responses to cyberviolence.

STOP! Child Sexual Exploitation
http://www.npa.go.jp/safetylife/syonen/no_cp/measures/index_e.html

The Protection of Human Rights (see pp.25-26)
http://www.moj.go.jp/content/001247391.pdf

5.5.13 Liechtenstein

Summaries or extracts of domestic legal provisions regarding cyberbullying, cyberstalking or other forms of cyberviolence.

Liechtenstein law has up to now no separate law or separate articles in the penal code concerning cyberbullying, cyberstalking or cyber mobbing. The Ministry of Justice of Liechtenstein is currently in the process of amending the Criminal Code. In the course of this amendment, a specific article (§107c) on "Cybermobbing" should be introduced into the criminal code. However, there are numerous criminal law provisions that can be used in cases such as cyberbullying, cyberstalking and other forms of cyberviolence:

Criminal Code

§ 105 - Coercion
1) Any person who coerces another person to do, acquiesce in or omit to do an act by force or a dangerous threat shall be punished with imprisonment of up to one year.
2) The act shall not be unlawful if the use of force or threat, as a means for the in-tended purpose, does not contradict common decency.

§ 106 - Aggravated coercion
1) Any person who commits coercion by
1. threatening death, substantial mutilation or conspicuous disfigurement, kidnapping, arson, endangerment through nuclear energy, ionizing radiation, or explosives, or destruction of livelihood or social status,
2. inflicting a state of agony on the coerced person or another person against whom the force or dangerous threat is directed, by these means and for an extended period of time, or
3. inducing the coerced person into marriage, registration of a partnership, prostitution, or participation in a pornographic performance (§ 215a paragraph 3), termination of pregnancy (§ 96) or otherwise into an act, acquiescence, or omission that violates particularly important interests of the coerced person or a third party shall be punished with imprisonment of six months to five years.
2) The perpetrator shall be punished likewise if the act results in the suicide or attempted suicide of the coerced person or of another person against whom the force or dangerous threat is directed.

§ 107 - Dangerous threat
1) Any person who threatens another person in a dangerous manner in order to scare and agitate such other person shall be punished with imprisonment of up to one year.
2) Any person who makes a dangerous threat by threatening death, substantial mutilation or conspicuous disfigurement, kidnapping, arson, endangerment through nuclear energy, ionizing radiation, or explosives, or destruction of livelihood or social status or who, by these means and for an extended period of time, inflicts a state of agony on the coerced person or another person against whom the force or dangerous threat is directed shall be punished with imprisonment of up to three years.
3) In the cases referred to in § 106 paragraph 2, the penalty set out there in shall be imposed.

§ 107a - Persistent stalking
1) Any person who unlawfully and persistently stalks another person (paragraph 2) shall be punished with imprisonment of up to three years.
2) A person persistently stalks another person if such person, in a manner capable of causing unreasonable interference with the lifestyle of such other person, for an extended period of time continuously
1. establishes physical proximity with such other person,

2. establishes contact with such other person by means of electronic communication or by use of other means of communication or through third parties,
3. orders merchandise or services for such other person and, for this purpose, uses such other person's personal data, or
4. causes third parties to contact the other person and, for this purpose, uses such other person's personal data.

§ 111 - Defamation
1) Any person who accuses another person of a despicable trait or attitude, of dishonourable conduct, or of any conduct in violation of common decency and does so in a manner that such accusation is perceivable by a third party and in a manner capable of defaming or degrading such other person in the public opinion shall be punished with imprisonment of up to six months or with a monetary penalty of up to 360 daily rates.
2) Any person who commits the act in a printed work, on the radio, on television, or in any other manner that causes the defamation to become accessible to the general public, shall be punished with imprisonment of up to one year or with a monetary penalty of up to 360 daily rates.
3) The perpetrator shall not be punished if the assertion is proven to be true. In the case set out in paragraph 1, the perpetrator shall not be punished either if evidence is provided of circumstances that gave the perpetrator sufficient ground to believe that the allegation was true.
4) Any evidence of truthfulness and any evidence of good faith shall be taken only if the perpetrator relies on the truthfulness of the assertion or on his good faith. No evidence of truthfulness and no evidence of good faith shall be allowed in relation to facts concerning private and family life or in relation to offences that can only be prosecuted upon demand of a third party. Likewise, no evidence of truthfulness and no evidence of good faith shall be allowed in relation to facts and assertions mainly put forward or disseminated with the purpose of accusing another person of disreputable things.

§ 112 - False accusation
1) Any person who accuses another person of a despicable trait or attitude, of dishonourable conduct, or of any conduct in violation of common decency and does so in a manner that the accusation is perceivable by a third party and in a manner capable of defaming or degrading such other person in the public opinion shall, if he knows (§ 5 paragraph 3) that the suspicion is untrue, be punished with imprisonment of up to two years or with a monetary penalty of up to 360 daily rates.
2) Any person who commits the act in a printed work, on the radio, on television, or in any other manner that causes the false accusation to become accessible to the general public, shall be punished with imprisonment of up to three years or with a monetary penalty of up to 360 daily rates.

§ 115 - Insult
1) Any person who insults or mocks another person, causes physical abuse to another person or threatens another person with physical abuse and does so in a manner perceivable to a third party, shall be punished with imprisonment of up to one month or with a monetary penalty of up to 60 daily rates, unless this act carries a more severe penalty under another provision.
2) Any person who commits the act set out in paragraph 1 in public or in front of several people shall be punished with imprisonment of up to three months or with a monetary penalty of up to 180 daily rates, unless this act carries a more severe penalty under another provision.
3) An act is committed in front of several people, if it is committed in front of more than two persons different from the perpetrator and the person attacked and if these are able to perceive the act.
4) Any person who is carried away only by outrage over the conduct of another person and as a consequence insults or physically attacks or threatens to physically attack another person in a manner exculpable in the circumstances shall be exculpated, if his outrage is generally understandable, in particular also with regard to the time that has passed since the event that triggered it.

§ 118a - Illegal access to a computer system
1) Any person who, with the purpose of obtaining knowledge, for himself or for another unauthorized person, of data stored on a computer system and not intended for him, and any person who, with the purpose of procuring a pecuniary benefit for himself or another person or of inflicting a disadvantage upon another person by using the data himself, making the data accessible to another person for whom the data is not intended or by publishing the data, gains access to a computer system that is not at his disposal or not at his sole disposal, or gains access to part of such a computer system, by overcoming specific security precautions in the computer system, shall be punished with imprisonment of up to six months or with a monetary penalty of up to 360 daily rates.
2) The perpetrator shall only be prosecuted with the authorization of the aggrieved party.
3) Any person who commits the act as a member of a criminal group shall be punished with imprisonment of up to three years.

§ 126a - Damage to data
1) Any person who causes damage to another by changing, deleting, or otherwise making unusable or suppressing data that is processed, transmitted, or supplied with the help of automation and that is not at his disposal or not at his sole disposal shall be punished with imprisonment of up to six months or with a monetary penalty of up to 360 daily rates.
2) Any person who through the act causes damage to the data in an amount exceeding 5,000 francs shall be punished with imprisonment of up to two

§ 126b - Interference with the functioning of a computer system
1) Any person who seriously interferes with the functioning of a computer system that is not at his disposal or not at his sole disposal by entering or transmitting data shall be punished with imprisonment of up to six months or with a monetary penalty of up to 360 daily rates, if the act does not carry a penalty pursuant to § 126a.
2) Any person who through the act brings about interference with the functioning of a computer system that persists for an extended period of time shall be punished with imprisonment of up to two years or with a monetary penalty of up to 360 daily rates; any person who commits the act as a member of a criminal group shall be punished with imprisonment of six months to five years.

§ 126c - Improper use of computer programmes or access data
1) Any person who develops, launches, distributes, alienates, otherwise makes accessible, procures or possesses
1. a computer programme which given its particular nature has been evidently developed or adapted to commit the act of obtaining illegal access to a computer system (§ 118a), to violate the secrecy of communication (§ 119), to commit the act of an improper interception of data (§ 119a), to cause damage to data (§ 126a), to cause interference with the functioning of a computer system (§ 126b), or to commit a fraudulent misuse of data processing (§ 148a), or any comparable device of this kind, or
2. a computer password, an access code, or comparable data that enables total or partial access to a computer system,
and does so with the intent to use them to commit any of the offences set out in subparagraph 1 shall be punished with imprisonment of up to six months or with a monetary penalty of up to 360 daily rates.
2) No person shall be punished in accordance with paragraph 1 if such person voluntarily prevents that the computer programme or comparable device referred to in paragraph 1 or the password, access code, any data comparable thereto be used in any of the manners set out in § 118a, § 119, § 119a, § 126a, § 126b or § 148a. If there is no danger of any such use or if such danger has been eliminated without any contribution by the perpetrator, the perpetrator shall not be punished if, not having any knowledge thereof, he voluntarily and earnestly endeavours to eliminate such danger.

§ 144 Extortion
1) Any person who by force or a dangerous threat coerces another person into an act, acquiescence, or omission that causes damage to the assets of such other person or of a third person shall be punished with imprisonment of six months to five years, if he acted with the intent to unjustly enrich himself or a third party through the conduct of the coerced person.
2) The act shall not be unlawful if the use of force or threat, as a means for the intended purpose, does not contradict common decency.

§ 148a Fraudulent misuse of data processing
1) Any person who, with the intent to unjustly enrich himself or a third party, causes damage to the assets of another person by influencing the results of automatic data
processing by designing the programme, by entering, changing, deleting, or suppressing data, or by otherwise intervening in the flow of the processing procedure shall be punished with imprisonment of up to six months or with a monetary penalty of up to 360 daily rates.
2) Any person who commits the act on a commercial basis or through the act causes damage in an amount exceeding 5,000 francs shall be punished with imprisonment of up to three years. Any person who through the act causes damage in an amount exceeding 75,000 francs shall be punished with imprisonment of one to ten years.

§ 218a Pornography
1) Any person who offers, displays, passes on, otherwise makes accessible or disseminates on the radio, on television or via other electronic media pornographic written materials, audio or video recordings, images, other objects of this kind or pornographic presentations of another person that has not yet reached the age of sixteen shall be punished with imprisonment of up to six months or with a monetary penalty of up to 360 daily rates.
2) Any person who publicly exhibits or shows objects or presentations within the meaning of paragraph 1 or otherwise offers them to another person without having been asked to do so shall be punished with imprisonment of up to three months or with a monetary penalty of up to 180 daily rates. Any person who in advance draws the attention of visitors to indoor exhibitions or indoor presentations to the pornographic character thereof shall not be punished.
3) Any person who produces, imports, stores, brings into circulation, advertises, exhibits, offers, displays, passes on or makes accessible objects or presentations within the meaning of paragraph 1 the content of which includes sexual acts with animals, human excreta or violent acts shall be punished with imprisonment of up to two years.
4) Any person who procures or possesses objects or presentations within the meaning of paragraph 1 the content of which includes violent acts shall be punished with imprisonment of up to one year.
5) Any person who commits the acts set out in paragraphs 1 to 3 on a commercial basis or as the member of a criminal group shall be punished with imprisonment of up to three years.
6) Objects or presentations for the purpose of this provision shall not be deemed pornographic if they have a cultural or scientific value worthy of protection.

§ 219 - Pornographic depictions of minors
1) Any person who
1. produces,
2. procures or possesses, or
3. offers, procures, passes on, presents, or makes accessible in any other manner to another person,
a pornographic depiction of a minor shall be punished with imprisonment of up to three years.
2) Any person who produces, imports, transports, or exports a pornographic depiction of a minor (paragraph 5) for the purpose of dissemination or who commits an act referred to in paragraph 1 on a commercial basis shall be punished with imprisonment of up to five years.
3) Any person who commits the act as a member of a criminal group or in such a manner that it results in a particularly severe disadvantage to the minor shall be punished with imprisonment of one to ten years; any person shall be punished likewise who produces a pornographic depiction of

a minor (paragraph 5) with use of severe force or who intentionally or grossly negligently endangers the life of the depicted minor when producing the pornographic depiction.
4) Any person who by means of information or communications technologies knowingly accesses a pornographic depiction of minors shall be punished with imprisonment of up to two years.
5) The following shall be deemed pornographic depictions of minors:
1. images or pictorial representations of a sexual act on a minor or of a minor on himself, on another person, or with an animal,
2. images or pictorial representations of the genitalia or the pubic region of minors, to the extent they are images reduced to the image itself and separated from other expressions of life, serving to sexually arouse the spectator.
6) Any person who produces or possesses a pornographic depiction of an adolescent with the adolescent's consent and for the adolescent's own use shall not be punished in accordance with paragraph 1(1) and (2).
7) Objects or presentations for the purpose of this provision shall not be deemed pornographic if they have a cultural or scientific value worthy of protection.

Data Protection Act
Article 39 Unauthorised collection of personal data
Whoever collects sensitive personal data without authorisation from a file which is not freely accessible shall at the request of the injured party be punished by the Landgericht (Court of Justice) for misdemeanour by imprisonment for up to one year or by a fine of up to 360 daily rates.

Links to domestic policies, strategies or responses to cyberviolence.

- The National Police of Liechtenstein runs a campaign to inform young adults and their parents about Internet criminality and Cybermobbing. The brochures aim to inform the young adults and the parents about the topic, explain what is legal and what not and give instructions on what to do if you encounter such criminal acts (only in German):

Cybermobbing: http://www.landespolizei.li/Portals/0/brosch%C3%BCren/11.pdf

Pornography: http://www.landespolizei.li/Portals/0/docs/pdf-Files/END%20porno_li_web.pdf

Harassment (for parents): http://www.landespolizei.li/Portals/0/docs/pdf-Files/safebook_eltern_liechtenstein.pdf

Harassment (for young adults): http://www.landespolizei.li/Portals/0/docs/pdf-Files/safebook_kinder_liechtenstein.pdf

Violence: http://www.landespolizei.li/Portals/0/docs/pdf-Files/Flyer_Handy-Gewalt.pdf

Stalking: http://www.landespolizei.li/Portals/0/docs/pdf-Files/stalking_li_extern1_end.pdf

- In 2014 the Government of Liechtenstein decided to establish an expert group on media competences that coordinates the various institutions and actors in the field of youth protection and social media. The expert group is on one side a point of contact for persons with questions and problems regarding new media an on the other side informs the public actively about the dangers in cyberspace. One of the topics the expert group covers is "Cyber-mobbing":
http://www.medienkompetenz.li/home.html

- In 2016 the expert group on media competences started a new prevention program that convey information about digital media, Cybermobbing, Cybergrooming, Sexting, Data protection in an interactive and age-appropriate way:
http://www.angeklickt.li/

5.5.14 Mauritius

Mauritius has developed a National Cyber Security Strategy policy for the years 2014-2019[116]. In the general framework of this policy, the National Computer Board issued a Guideline on Social Network[117] and a booklet entitled "Online Responsible Choice for Youngster"[118].

The latter document contains some interesting considerations on combating cyberbullying and cyberviolence, focusing on the idea of respecting the rights of others online, especially human rights.

In particular, the rights are summarised in the followings:

1. **Be safe!** You might not experience physical violence online, but you might experience mental and emotional violence or harassment. You have the right to be free from all types of violence and harassment.
2. **Have fun!** You might not realise it, but you have the right to have fun. There is a human right that says that you have the right to leisure and play. People that are being bullied may feel like they cannot spend time with their friends and enjoy themselves like everyone else. So remember, you have the right to have fun safely at school, in public or online!
3. **Be healthy!** An important human right is the right to a good standard of physical and mental health. This means that you have a right to have health care. It also means that you have a right to be free from other people's behaviour that may hurt your health. Cyberbullying can be extremely distressing and may cause physical and mental injuries, such as anxiety and depression.
4. **Privacy!** People who are cyberbullied might have their personal information put online or sent by phone for everyone to see. This includes texts and photos that are hurtful and embarrassing. If this is done without permission your right to privacy is not being respected.
5. **Get an education!** Cyberbullying can make people feel unsafe and unwelcome at school. We all have the right to education and should be able to go to school without being worried about our safety and to know more about cyberbullying.
6. **Have a say!** You have the right to express your feelings and have your say! People who are bullied may feel like they can't express themselves as they are worried and scared. So remember; both online and offline you have the right to have your voice heard as long as you are respectful of yourself and others!
7. **Work safely!** If you are old enough to have a job you also have the right to work and fair working conditions. This means that your work-place should be safe and be free from cyberbullying.

The booklet calls for a shared responsibility to avoid that anyone can be bullied online. Cyberbullying is everyone's concern and it is important that everyone is part of the solution, not the problem.

Finally, there is a call for tolerance on others opinion when published online.

5.5.15 Mexico

116 http://mtci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf (link checked last 18th of July 2017)

117 http://cybersecurity.ncb.mu/English/Documents/Knowledge%20Bank/Guidelines/Guideline%20on%20Social%20Networks.pdf (link checked last 18th of July 2017).

118 http://www.ncb.mu/English/Documents/Booklet/Prefinal%20Booklet.pdf (link checked last 18th of July 2017).

Federal Criminal Code (Federal legislation enforced across the country) contains provisions on prosecution of:

Chapter II. Pornography of Persons under the Age of Eighteen or Persons who do not have the capacity to understand the Meaning of the Fact or of Persons who do not have the Capacity to Oppose.

Article 202. Commits the crime of pornography of persons under the age of eighteen or of persons who do not have the capacity to understand the meaning of the act or of persons who do not have the capacity to oppose to it, the persone who procure, oblige, facilitate or induce, for any means, to one or more of these persons to perform sexual acts or body exhibitionism with lascivious or sexual purposes, real or simulated, for the purpose of video recording, photographing, filming, displaying or describing them through printed advertisements, transmission of data files in public or private telecommunications networks, computer systems, electronics or substitutes. The perpetrator of this crime will be sentenced to seven to twelve years in prison and a fine of eight hundred to two thousand days.

Whoever fixes, prints, records, photographs, films or describes physical or lascivious or sexual acts, real or simulated, involving one or more persons under the age of eighteen or one or more persons who do not have the capacity to understand the meaning of the event or one or more people who have no ability to oppose, will be imposed the penalty of seven to twelve years in prison and eight hundred to two thousand days fine, as well as the seizure of objects, instruments and products of the crime.

The same penalty shall be imposed on anyone who reproduces, stores, distributes, sells, purchases, leases, exhibits, advertises, transmits, imports or exports the material referred to in the preceding paragraphs.

Article 202 BIS.- Anyone who stores, buys, leases, the material referred to in the preceding paragraphs, without marketing or distribution purposes will be imposed one to five years in prison and a fine of one hundred to five hundred days. Furthermore the person will also may be subject to specialized psychiatric treatment.

General Law to Prevent, Punish and Eradicate Crimes related to Human Trafficking and for Protection and Assistance to the Victims of these Crimes

Of crimes in the area of Human Trafficking

Article 10.- Any act or intentional omission of one or more persons to capture, engage, transport, transfer, retain, deliver, receive or lodge one or more persons for the purpose of exploitation will be imposed from 5 to 15 years in prison and from a thousand to twenty thousand days fine, without prejudice to the corresponding sanctions for each one of the crimes committed, foreseen and sanctioned in this Law and in the corresponding penal codes.

It will be understood as exploitation of a person to:
…

III. The prostitution of others or other forms of sexual exploitation, in the terms of articles 13 to 20 of this Law;

Article 13. Shall be sanctioned with a penalty of imprisonment from 15 to 30 years and a fine of one thousand to 30 thousand days whoever benefits from the exploitation of one or more persons through prostitution, pornography, public or private exhibitions of a sexual nature, sex tourism or any other sexual activity paid by:

I. Deception;
II. Physical or moral violence;
III. The abuse of power;
IV. The abuse of a situation of vulnerability;
V. Serious damage or threat of serious harm; or
VI. The threat to report to authorities about their immigration status in the country or any other abuse of the use of law or legal proceedings, which causes that the passive subject decide to submit to the requirements of the perpetrator.

In the case of minors or persons who do not have the capacity to understand the meaning of the event, the verification of the means referred to in this article will not be required.

Article 16. Shall be punished with a penalty of imprisonment from 15 to 30 years in prison and a fine of 2 thousand to 60 thousand days, as well as confiscation of the objects, instruments and proceeds of crime, including the destruction of the resulting materials, anyone who procure, promotes, oblige, advertise, manage, facilitate or induce, by any means, a person under the age of eighteen, or a person who does not have the capacity to understand the meaning of the act, or has no the capacity to resist the conduct, to perform sexual acts or body exhibition, for sexual purposes, real or simulated, in order to produce material through video record, audio record, photograph, film, display or to describe it through printed ads, computer systems, electronics or substitutes, and benefit economically from the exploitation of the person.

If the use of force, deception, physical or psychological violence, coercion, abuse of power or a situation of vulnerability, addictions, a hierarchical or trusting position, or the granting or receipt of payments or benefits were made to obtain the consent of a person who has authority over another or any other circumstance that diminishes or eliminates the will of the victim to resist, the penalty foreseen in the previous paragraph will be increased by one half.

The same sanctions foreseen in the first paragraph of this article will be imposed, to whoever finances, elaborates, reproduces, stores, distributes, commercializes, leases, exposes, publicizes, disseminates, acquires, exchanges or shares, by any means, the material to which the previous behaviors refer.

Article 17. A penalty with imprisonment from 5 to 15 years and a fine of one thousand to 20 thousand days will be imposed on anyone who stores, acquires or leases for himself or for a third party, the material referred to in the previous article, without marketing purpose or distribution.

Article 18. Shall be punished with a penalty of imprisonment from15 to 25 years and a fine of one thousand to 20 thousand days anyone who promotes, advertises, invites, facilitates or manages by any means one or more persons to travel to the national territory or abroad with the purpose of performing any type of sexual acts, real or simulated, with one or more persons under the age of eighteen, or with one or several persons who have no capacity to understand the meaning of the act or with one or several people who do not have the capacity to resist it, and benefit economically from it.

5.5.16 Moldova

In the national legislation, the Republic of Moldova has no regulation of cyberbullying, cyberstalking or other forms of cyberviolence.
Facts of psychological violence, threats, including life threats and health threats, are qualified according to special articles of the Criminal Code or Code of offenses.

5.5.17 Norway

Norway's population has a high level of access and use of technology and the internet. A large majority of the population use social media, with 86% using Facebook daily. According to a survey by the Norwegian Media Authority (NMA)[119], nearly all Norwegian children above the age of 10 have access to a smart phone and use it every day for social media, games and video streaming services, with Snapchat being the most popular service for children and youth (2017). More than 1 out of 4 children between 9- 18 years old, report that they have experienced bullying or being harassed in some way through internet services, games or mobile devices. 13 % of 13 - 18 year olds report that they have sent a nude picture. The numbers are on the same level as in 2016 for youth above 15 years, but shows some increase for children who are 13 -14 years. Almost 2 out of 10 says that they have received unpleasant, offensive or threatening sexual comments online. Many children and youth will not report what they have experienced, due to feeling ashamed or having fears that they will no longer be allowed to use their mobile.

Norwegian police describes an alarming development concerning online child abuse, with several large cases indicating the magnitude and complexity of this type of crime. Technological developments with high resolution video and pictures, as well as direct videochat, facilitates sexualised contact with children. Moreover, one perpetrator easily reaches and can manipulate a very high number of victims through online channels. The National Criminal Investigation Service (Kripos) observed approximately 3000 unique IP-addresses 2016 - 2017 used for downloading or sharing child abuse material. Furthermore, the police has also noted that an increasing amount of such material is available on the dark net[120].

In 2016 the Norwegian government launched an Escalation Plan against violence and abuse (2017-2021), containing increased budgets as well as a stronger focus on online child abuse. The efforts also include knowledge development concerning online risks for children (EU Kids Online, data collection 2018). Online child abuse is highlighted as a priority area in relevant central annual steering documents from the government and funds have been earmarked for the National Criminal Investigation Service (NCIS) to develop the work against child abuse. Recent reform of the organisation of Norwegian police will improve the ability to tackle the comprehensive challenges. Also, the National Police Directorate has in 2018 started the establishment of a National Cybercrime Centre (NC3) with the purpose of coordinating and supporting national and cross-border cybercrime law enforcement activities and act as a centre of technical expertise. On a more concrete note, NCIS initiated in 2017 the launch of concerted action, called "Police2Peer", targeting perpetrators who are sharing child abuse material through peer-to-peer networks, stating a good example of an innovative approach to the challenges. The central objectives are to increase police presence where child abuse material is shared, increase the perceived risk of being apprehended and ultimately decrease the demand and availability of child abuse material. The

119 Survey from The Norwegian Media Authority 2018 Barn og medier-undersøkelsen (http://www.medietilsynet.no/globalassets/dokumenter/trygg-bruk/barn-og-medier-2018/delrapporter-barn-og-medier-2018/barn-og-medier-2018-mobbing-ubehagelige-opplevelser-og-rapportering.pdf
http://www.medietilsynet.no/globalassets/dokumenter/trygg-bruk/barn-og-medier-2018/delrapporter-barn-og-medier-2018/barn-og-medier-2018--seksuelle-kommentarer-og-deling-av-nakenbilder.pdf)

120 Report from the Norwegian police Trusler og utfordringer innen IKT-kriminalitet. https://www.politiet.no/globalassets/dokumenter/pod/ikt_krim_pod.pdf

project was presented during the twenty-seventh session of the Commission on Crime Prevention and Criminal Justice in Vienna in May 2018.

With an aim to prevent risks and harm of children online, relevant ministeries have been supporting the Norwegian Media Authority (NMA) through the EU co-funded Safer Internet programme and the Norwegian National Awareness Centre since 2006. As the national Awareness Centre, NMA have encouraged cooperation and dialogue between industry, educators, governmental bodies and NGOs and more specifically the role of providing Safer Internet Services in collaboration with the Norwegian Red Cross Helpline (Røde kors/Kors på halsen). Of significant importance is the collaboration that NMA/the Safer Awareness Centre Norway (Trygg bruk) has with the Norwegian NCIS, National Criminal Investigation Service (Kripos), on issues related to sexual exploitation of children. The NCIS has the function and role of a national hotline concerning reports on child abuse material. An important objective is to ensure effective action towards online child abuse through cross-sector cooperation, a solid knowledge base and sufficient resources and capacities. Overall, many actors and levels need to be coordinated and agree on priorities and sharing of responsebilities to address the challenges. Also, combatting child abuse online goes beyond the national context, thus it is instrumental to provide an international arena for discussion and initiation of action and collaboration.

Noteworthy initiatives are the services of SlettMeg.no ("DeleteMe"), assisting the public to get in touch with various internet and social media providers to remove unwanted content, the initiative "Bruk Hue" ("Use your head") raising awareness by visiting schools.

Threats and online harassment towards adults online are generally followed up by the police in individual cases. In several cases, prosecutors and courts have issued restraining orders that included contact online, including via e-mail and social media. The legal instruments regarding restraining orders and violation of these, do not mention internet and social media specifically, but according to Norwegian legal practices, this is not required. In a recent Supreme Court case (HR-2016-2263-A), a man was convicted for assisting in distribution of a large number of images of private nature (via BitTorrent). The images had been retrieved from social media, where most of them had been posted by the women themselves, as they trusted the pictures would not and could not be disseminated. In the file sharing application, the images were sorted in such a way that many of the women could easily be identified. The judgment emphasised the need for a general deterrent and a central part of the legal arguments, were the Copyright Act Section 45 c a provision regulating consent for use of photos.

From the Supreme Court decision: "The women themselves did not know that pictures of them were circulating on the Internet. Consequently, they did not consent to the pictures' use. (…) The right to determine the use of one's own photographs also clearly has to do with privacy protection. (…) In the Official Norwegian Reports 2007:2 item 3.7.4 (about personal pictures on the net) highlights section 45 c as a key provision which will particularly have bearing on unwanted and illegal publication of such pictures on the net. The provision does not only defend financial interests, as some opinions expressed in the act's preparatory works". In another recent case, the Supreme Court set aside a conviction for distribution of private photos of sexual nature (HR-2017-1245-A). In this case, the charge was violation of Section 201 in the General Civil Penal Code of 1902 (sexually offensive or otherwise indecent behaviour in the presence of or towards any person who has not consented). In this case, a man had taken photos of a young woman during sexual activity, and shared the documentation with several others. The conviction in the Appeals Court was set aside by the Supreme Court; the photos in question were not shared "towards" the victim, so the facts of the case were not covered by the charges. The Supreme Courts also stated that the facts of the case may have been a violation of other articles in the Penal Code, but this was outside the charges. As of June 2018, it is not clear if there will be filed new charges in this case.

5.5.18 Slovakia

At present, there is no law in Slovakia that would define expressis verbis the concept of cyberbullying or cyberviolence. The current Slovak legislation does not define these terms. However, it does not mean that cyberbullying or other forms of cyberviolence through ITC, dissemination of intimate images or child luring (for instance for the purposes of sexual exploitation) do not have any legal consequences. For such actions, several provisions of the Criminal Code (No. 300/2005 Coll. as amended, hereinafter referred to as *"CC"*) can be applied, namely:

- Stalking (Section 360a of CC)
- Extortion (Section 189 of CC)
- Duress (Section 192 of CC)
- Sexual Exploitation (Section 201, Section 201a, Section 201b of CC)
- Defamation (Section 373 of CC)
- Harm Done to Rights of Another (Section 375, 376 of CC)
- Manufacturing of child pornography (Section 368 of CC)
- Dissemination of child pornography (Section 369 of CC)
- Possession of child pornography and Participation in Child Pornographic Performance
- Corrupting Morals (Sections 371, 372 of CC)
- Corrupting Morals of Youth (Section 211 of CC)
- Establishment, Support and Promotion of Movements Directed at the Suppression of Fundamental Rights and Freedoms (Section 421 of CC)
- Expression of Sympathy for Movements Directed at the Suppression of Fundamental Rights and Freedoms (Section 422 of CC)
- Production, Distribution, Possession of Extremist Materials (Sections 422a, 42 2b, 422c of CC)
- Denial and Approval of the Holocaust, the Crimes of Political Regimes and the Crimes against Humanity (Section 422d of CC)
- Defamation of Nation, Race and Conviction (Section 423 of CC)
- Incitement to National, Racial and Ethnic Hatred (Section 424 of CC)

Section 360a
Stalking
(1) Whoever follows another person over an extended period of time in a way giving possible rise to a reasonable fear for the life or health of that person or the life or health of a person close to that person or giving rise to the substantial impairment of the quality of life of that person by
a) threatening to inflict bodily harm or other harm to that person or a person close to that person,
b) seeking the personal proximity of that person or following that person,
c) contacting that person through a third person or electronic communication service, in writing or in any other manner against the will of that person,
d) misusing the personal details of that person in order to establish personal or any other contact with that person, or
e) limiting that person in their usual way of life, shall be punished by a prison sentence of up to one year.

(2) A prison sentence of six months to three years shall be imposed upon an offender if they committed an act referred to in Subsection 1
a) against a protected person,
b) in a more serious manner of conduct,
c) out of a special motive, or
d) publicly.

Section 189
Extortion
(1) Any person who forces another person by violence, the threat of violence or the threat of other serious harm to do anything, omit doing or endure anything being done shall be liable to a term imprisonment of two to six years.
(2) The offender shall be liable to a term of imprisonment of four to ten years if he commits the offence referred to in paragraph 1
a) acting in a more serious manner,
b) against a protected person,
c) by reason of specific motivation, or
d) and causes larger damage through its commission.
(3) The offender shall be liable to a term of imprisonment of ten to twenty years if he commits the offence referred to in paragraph 1,
a) and causes grievous bodily harm or death through its commission, or
b) and causes substantial damage through its commission.
(4) The offender shall be liable to a term of imprisonment of twenty to twenty-five years or to life imprisonment if he commits the offence referred to in paragraph 1,
a) and causes grievous bodily harm or death to several persons through its commission,
b) and causes large-scale damage through its commission, or
c) as a member of a dangerous grouping.

Section 192
Duress
(1) Any person who, by taking advantage of another person's material distress or pressing need of other than proprietary nature, or pressure provoked by his adverse personal situation, forces such person without lawful authority to do, omit doing or endure something being done shall be liable to a term of imprisonment of up to three years.
(2) The offender shall be liable to a term of imprisonment of one to five years if he commits the offence referred to in paragraph 1
a) acting in a more serious manner,
b) against a protected person,
c) by reason of specific motivation,
d) with the intention to obtain larger property benefit or other benefit for himself or another, or
e) by denying an employee in an employment relation or a similar working relation to exercise his right to safe and healthy working conditions, to annual leave or to the creation of statutory working conditions for women and juvenile workers.
(3) The offender shall be liable to a term of imprisonment of four to ten years if he commits the offence referred to in paragraph 1,
a) and causes grievous bodily harm or death through its commission, or
b) and causes substantial damage through its commission.
(4) The offender shall be liable to a term of imprisonment of ten to twenty-five years or to life imprisonment if he commits the offence referred to in paragraph 1,
a) and causes large-scale damage through its commission,
b) and causes death to several persons through its commission,
c) as a member of a dangerous grouping, or
d) under a crisis situation.

Sexual Abuse
Section 201
(1) Any person who has sexual intercourse with a person under fifteen years of age, or who subjects such person to other sexual abuse, shall be liable to a term of imprisonment of three to ten years.
(2) The offender shall be liable to a term of imprisonment of seven to twelve years if he commits the offence referred to in paragraph 1
a) acting in a more serious manner, b) against a protected person, or

c) by reason of specific motivation.
(3) The offender shall be liable to a term of imprisonment of twelve to fifteen years if he commits the offence referred to in paragraph 1, and causes grievous bodily harm through its commission.
(4) The offender shall be liable to a term of imprisonment of fifteen to twenty years if he commits the offence referred to in paragraph 1,
a) and causes death through its commission, or
b) under a crisis situation.

Section 201a
Whoever, using an electronic communication service, proposes a personal meeting to a child below fifteen years of age with the intention to commit a criminal offence of sexual abuse or a criminal offence of production of child pornography against them and is not a child themselves, shall be punished by a prison sentence of six months to three years.

Section 201b
Whoever misuses a child below fifteen years of age with the intention to achieving sexual satisfaction by such child's participation in sexual activities or sexual abuse, without such child having to necessarily take part in such sexual activities or sexual abuse, or whoever makes such abuse of a child possible, shall be punished by a prison sentence of up to two years.

Section 373
Defamation
(1) Any person who communicates a false information about another likely to considerably damage the respect of fellow citizens for such a person, damage his career and business, disturb his family relations, or cause him other serious harm, shall be liable to a term of imprisonment of up to two years.
(2) The offender shall be liable to a term of imprisonment of one to five years if he commits the offence referred to in paragraph 1,
a) and causes substantial damage through its commission,
b) by reason of specific motivation.
c) in public, or
d) in business acting in a more serious manner.
(3) The offender shall be liable to a term of imprisonment of three to eight years if he commits the offence referred to in paragraph 1,
a) and causes large-scale damage through its commission, or
b) and causes another to lose his job, collapse his undertaking or divorce his marriage.

Section 375
Harm Done to Rights of Another
(1) Any person who causes serious prejudice to the rights of another by
a) misrepresentation of another or
b) taking advantage of mistake of another
shall be liable to a term of imprisonment of up to two years.
(2) The offender shall be liable to a term of imprisonment of between six months and three years if he commits the offence referred to in paragraph 1
a) acting in a more serious manner,
b) against a protected person, or
c) by pretending to be a public official.
(3) The offender shall be liable to a term of imprisonment of one to five years if he commits the offence referred to in paragraph 1, and obtains substantial benefit for himself or another through its commission.

Section 376
Any person who unlawfully breaches the secrecy of an instrument or other written document, audio recording, video recording or other recording, computer data or other document kept private

by another through disclosing them or making them accessible to a third person, or using them otherwise, and thus causes serious prejudice to the rights of another, shall be liable to a term of imprisonment of up to two years.

Section 368
Manufacturing of Child Pornography
(1) Any person who exploits, elicits, offers or otherwise abuses a child for manufacturing child pornography, or enables such abuse of a child, or otherwise participates in such manufacturing, shall be liable to a term of imprisonment of four to ten years.
(2) The offender shall be liable to a term of imprisonment of seven to twelve years if he commits the offence referred to in paragraph 1
a) against a child under twelve years of age,
b) acting in a more serious manner, or
c) in public.
(3) The offender shall be liable to a term of imprisonment of ten to fifteen years if he commits the offence referred to in paragraph 1,
a) and causes grievous bodily harm or death through its commission, or
b) and obtains substantial benefit through its commission.
(4) The offender shall be liable to a term of imprisonment of twelve to twenty years if he commits the offence referred to in paragraph 1,
a) and causes grievous bodily harm or death to several persons through its commission,
b) and obtains large-scale benefit through its commission, or
c) as a member of a dangerous grouping.

Section 369
Dissemination of Child Pornography
(1) Any person who disseminates, transports, procures, makes accessible or otherwise puts into distribution child pornography shall be liable to a term of imprisonment of one to five years.
(2) The offender shall be liable to a term of imprisonment of three to eight years if he commits the offence referred to in paragraph 1
a) acting in a more serious manner, or
b) in public.
(3) The offender shall be liable to a term of imprisonment of four to ten years if he commits the offence referred to in paragraph 1, and obtains substantial benefit through its commission.
(4) The offender shall be liable to a term of imprisonment of seven to twelve years if he commits the offence referred to in paragraph 1, and obtains large-scale benefit through its commission.

Section 370
Possession of Child Pornography and Participation in a Child Pornographic Performance
(1) Whoever possesses child pornography or whoever acts with the intention to obtain access to child pornography through an electronic communication service shall be punished by a prison sentence of up to two years.

(2) The same punishment referred to in Subsection 1 shall be imposed upon a person who intentionally participates in child pornographic performance.

Section 371
Corrupting Morals
(1) Any person who manufactures, purchases, imports or otherwise procures and subsequently sells, rents or otherwise puts into distribution, disseminates, makes publicly accessible or publishes pornographic works, audio or video carriers, images or other objects corrupting morals, which show human beings with disrespect and display violence, or depict sexual intercourse with an animal, or other pathological sexual practices, shall be liable to a term of imprisonment of up to two years.

(2) The offender shall be liable to a term of imprisonment of one to five years if he commits the offence referred to in paragraph 1
a) acting in a more serious manner, or
b) in public.
(3) The offender shall be liable to a term of imprisonment of three to eight years if he commits the offence referred to in paragraph 1, and obtains substantial benefit through its commission.
Any person who
a) offers, surrenders or makes pornography accessible to a person under eighteen years of age, or
b) exhibits or otherwise makes pornography accessible to persons under eighteen years of age in a place accessible to such persons,
shall be liable to a term of imprisonment of up to two years.
(2) The offender shall be liable to a term of imprisonment of one to five years if he commits the offence referred to in paragraph 1
a) acting in a more serious manner, or
b) in public.
(3) The offender shall be liable to a term of imprisonment of three to eight years if he commits the offence referred to in paragraph 1, a) and obtains substantial benefit for himself or another, or
b) by offering, making available or exhibiting pornographic works, audio or video carriers or images, which show human beings with disrespect and display violence, or depict sexual intercourse with an animal, or other pathological sexual practices.

Section 211
Corrupting Morals of Youth
(1) Any person who, even by negligence, exposes a person under eighteen years of age to the risk of debauchery by
a) enticing such person to leading lewd or immoral life,
b) enabling such person to lead lewd or immoral life,
c) enabling such person to perform actions which are considered as criminal offences under this Act, or
d) preventing such person from compulsory school attendance,
shall be liable to a term of imprisonment of up to two years.
(2) The same sentence as referred to in paragraph 1 shall be imposed on the offender who, contrary to a generally binding legal regulation, employs a child under fifteen years of age, and thus prevents him from compulsory school attendance.
(3) The offender shall be liable to a term of imprisonment of between six months and five years if he commits the offence referred to in paragraphs 1 and 2
a) acting in a more serious manner, or
b) by reason of specific motivation.

Section 421
Establishment, Support and Promotion of Movements Directed at the Suppression of Fundamental Rights and Freedoms

(1) Whoever establishes, supports or promotes a group, movement or ideology which is directed at the suppression of the fundamental rights and freedoms of persons or which propagates racial, ethnic, national or religious hatred or hatred against another group of persons or whoever promotes a group, movement or ideology that was directed at the suppression of the fundamental rights and freedoms of persons in the past, shall be punished by a prison sentence of one to five years.
(2) An offender shall be punished by a prison sentence of four to eight years if they committed an act referred to in Subsection 1

a) publicly or in a publicly accessible place,
b) in a more serious manner of conduct, or
c) in a crisis situation.

Section 422
Expression of Sympathy for Movements Directed at the Suppression of Fundamental Rights and Freedoms
(1) Whoever, publicly or in a publicly accessible place, particularly by using flags, badges, uniforms or slogans, expresses sympathy for a group, movement or ideology which is directed or was directed in the past at the suppression of the fundamental rights and freedoms of persons or which propagates racial, ethnic, national or religious hatred or hatred against another group of persons, shall be punished by a prison sentence of six months to three years.
(2) The same punishment referred to in Subsection 1 shall be imposed upon a person who uses altered flags, badges, uniforms or slogans appearing to be genuine during the commission of an act referred to in Subsection 1.

Section 422a
Production of Extremist Materials
(1) Whoever produces extremist materials or is accessory to such production shall be punished by a prison sentence of three to six years.
(2) An offender shall be punished by a prison sentence of four to eight years if they committed an act referred to in Subsection 1
a) in a more serious manner of conduct, or
b) as a member of an extremist group.

Section 422b
Distribution of Extremist Materials
(1) Whoever copies, transports, procures, makes accessible, puts into circulation, imports, exports, offers, sells, ships or distributes extremist materials, shall be punished by a prison sentence of one to five years.
(2) A prison sentence of three to eight years shall be imposed upon an offender if they committed an act referred to in Subsection 1
a) in a more serious manner of conduct,
b) publicly, or
c) as a member of an extremist group.

Section 422c
Possession of Extremist Materials
Whoever possesses extremist materials shall be punished by a prison sentence of up to two years.

Section 422d
Denial and Approval of the Holocaust, the Crimes of Political Regimes and the Crimes against Humanity
(1) Whoever publicly denies, disputes, approves or tries to justify the holocaust, the crimes of a regime based on a fascist ideology, the crimes of a regime based on a communist ideology or crimes of a similar movement which through violence, threat of violence or threat of other grievous harm leads to the suppression of fundamental rights and freedoms of persons shall be punished by a prison sentence of six months to three years.
(2) The same punishment referred to in Subsection 1 shall be imposed upon a person who publicly denies, approves, doubts, seriously derogates or tries to justify genocide, crimes against peace, crimes against humanity or war crimes in a manner that may incite violence or hatred against a group of persons or a member of such a group, if the offender or an accessory to such an act was convicted by a final judgment of an international court established under international public law, the authority of which is recognised by the Slovak Republic, or by a final judgment of a court of the Slovak Republic.

Section 423
Defamation of Nation, Race and Conviction
(1) Whoever publicly defames
a) any nation, its language, any race or ethnic group, or
b) a group of persons or an individual because of their actual or deemed belonging to a race, nation, nationality, ethnicity, because of their actual or deemed origin, skin colour, political opinions, religion, or because they have no religion, shall be punished by a prison sentence of one to three years.
2) A prison sentence of two to five years shall be imposed upon an offender if they committed an act referred to in Subsection 1
a) as a member of an extremist group,
b) as a public official, or
c) out of a special motive.

Section 424
Incitement to National, Racial and Ethnic Hatred
(1) Whoever publicly incites violence or hatred against a group of persons or an individual because of their actual or deemed belonging to a race, nation, nationality, ethnicity, because of their actual or deemed origin, skin colour, sexual orientation, political opinions, religion, or because they have no religion, or whoever publicly incites restriction of their rights and freedoms, shall be punished by a prison sentence of up to three years.
(2) The same punishment referred to in Subsection 1 shall be imposed upon a person who plots or assembles to commit an act referred to in Subsection 1.
(3) A prison sentence of two to six years shall be imposed upon an offender if they committed an act referred to in Subsection 1 or 2
a) out of a special motive,
b) as a public official,
c) as a member of an extremist group, or
d) in a crisis situation.

5.5.19 Spain

BUDAPEST CONVENTION ARTICLES WITH A MORE-DIRECT CONNECTION TO CYBERVIOLENCE

5.5.19.1 ARTICLE 4 Data interference in a critical system

Article 264 Spanish Penal Code states:
1.Whoever, by any means, without authorisation and in a serious way, were to erase, damage, deteriorate, alter, suppress, or make data, computer programs or electronic documents pertaining to others inaccessible, if the result produced is serious, shall be punished with a prison sentence of six months to three years.

2. A prison sentence of two to five years and a fine of one to ten times the amount of damage caused shall be imposed, when any of the following circumstances concurs in the conduct described:
1. If committed within the setting of a criminal organisation;
2. If they cause particularly serious damage or damage that affects a large number of computer systems.
3. If the deed causes severe detriment to the operation of essential public services or the provision of goods of primary necessity;
4. If the deeds have affected the computer system of a critical infrastructure or have created a situation of serious danger for the security of the State, of the European Union or of a Member State of the European Union. To this effect, critical infrastructure shall be construed as an element, system or part thereof that is essential for the maintenance of the vital functions of society, health, security, protection and economic and social welfare of the population, the

disruption or destruction whereof would have a significant impact as a result of the failure to maintain such functions;
5. The criminal offence has been committed by using any of the means outlined in Article 264 ter.
If the deeds have produced extremely serious effects the higher degree penalty shall be imposed.

3. The penalties imposed shall be higher by one degree to those respectively stated in the previous Sections when the deeds are committed through the unauthorised use of the personal data of another person to provide access to the computer system or to secure the trust of a third party.

5.5.19.2 ARTICLE 5 System interference in a critical system

Article 264 bis Spanish Penal Code
1. Whoever, without authorisation and in a serious way, hinders or interrupts the operation of a computer system pertaining to another in any of the following manners shall be punished with a prison sentence of six months to three years:
a) By engaging in any of the conducts outlined in the preceding Article;
b) By introducing or transferring data, or;
c) By destroying, damaging, disabling, eliminating or substituting a computer or telematic system or of electronic data storage.
If the deeds were to significantly hinder the normal activity of a company, business or Public Administration, the penalty shall be imposed in its upper half and up to the highest degree.
2. If any of the circumstances outlined in Section 2 of the preceding Article concurs in the case of the deeds foreseen in the previous Section, a prison sentence of three to eight years and a fine of three to ten times the amount of the damage caused shall be imposed.
3. The penalties imposed shall be higher by one degree to those respectively stated in the previous Sections when the deeds are committed through the unauthorised use of the personal details of another person to provide access to the computer system or to secure the trust of a third party.

5.5.19.3 ARTICLE 9 - Child pornography

Article 189 Spanish Penal Code
1. A prison sentence of one to five years shall be handed down to:
a) Whoever recruits or uses minors or persons with disabilities requiring special protection for exhibitionistic or pornographic purposes or shows, both public or private, or to prepare any kind of pornographic material, whatever the medium, or who finances or profits from any of these activities;
b) Whoever produces, sells, distributes, displays, offers or facilitates the production, sale, diffusion or display by any medium of child pornography, or material for the preparation for which minors or persons with disabilities requiring special protection have been used, or possesses such material for such purposes, even though the material is of foreign or unknown origin.

For the purposes of this Title, child pornography, or that for the preparation whereof minors or persons with disabilities requiring special protection have been used, shall be considered as:
a) All material that visually displays a minor or a person with disabilities requiring special protection participating in a sexually explicit conduct, whether real or simulated;
b) Any display of the sexual organs of a minor or a person with disabilities requiring special protection for predominantly sexual purposes;
c) All material that visually displays a person who appears to be a minor participating in sexually explicit conduct, whether real or simulated, or any display of the sexual organs of a person who appears to be a minor, for predominantly sexual purposes, unless the person who appears to be a minor is actually eighteen years or older at the time of taking the images;
d) Realistic images of a minor participating in sexually explicit conduct or realistic images of the sexual organs of a minor, for predominantly sexual purposes.

2. Whoever perpetrates the deeds foreseen in Section 1 of this Article shall be punished with a prison sentence of five to nine years if any of the following circumstances concurs:
a) If using children under the age of sixteen years;
b) If the deeds are particularly degrading or humiliating in nature;
c) If the pornographic material displays minors or persons with disabilities requiring special protection who are victims of physical or sexual violence;
d) If the offender has endangered the life or health of the victim, intentionally or due to gross negligence;
e) If the deeds are especially serious in view of the financial value of the pornographic material;
f) If the culprit is a member of an organisation or association, even on a temporary basis, dedicated to carrying out such activities;
g) If the offender is an ascendant, tutor, carer, minder, teacher or any other person in charge, *de facto*, even on a provisional basis, or *de jure*, of the minor or person with disabilities requiring special protection, or any other member of the family who lives with him and who has abused his recognised position of trust or authority;
h) If the aggravating circumstance of recidivism concurs.
3. If the deeds outlined in Sub-Paragraph a) of the first Paragraph of Section 1 were committed with violence or intimidation, the higher degree punishment than those foreseen in the preceding Sections shall be imposed.

4. Whoever knowingly attends exhibitionistic or pornographic shows involving minors or persons with disabilities requiring special protection shall be punished with a prison sentence of six months to two years.
5. Whoever possesses or acquires child pornography for his own use, or material for the preparation whereof minors or persons with disabilities requiring special protection have been used, shall be punished with a prison sentence of three months to a year or with a fine of six months to two years.
The same sanction shall be imposed on individuals who knowingly access child pornography, or material for the preparation whereof minors or persons with disabilities requiring special protection have been used.
6. Whoever has a minor or person with disabilities requiring special protection under his care, guardianship, protection or fostership and who, being aware of his state of prostitution or corruption, does not do everything possible to prevent such situation continuing, or does not resort to the competent authority for such a purpose, if lacking the resources to safe keep the minor or person with disabilities requiring special protection, shall be punished with a prison sentence of three to six months or a fine of six to twelve months.
7. The Public Prosecutor shall promote the pertinent actions in order to deprive whoever commits any conduct described in the preceding Section of his parental rights, guardianship, safekeeping or family fostership, as appropriate.
8. Judges and Courts of Law shall order the adoption of the measures necessary to withdraw the websites or web applications that contain or distribute child pornography or those for the preparation whereof persons with disabilities requiring special protection have been used or, where appropriate, to block access to such websites or applications to Internet users who are within Spanish territory.
Such measures may be decreed on a precautionary basis at the request of the Public Prosecutor.

Article 183 ter Spanish Penal Code (grooming)
1. Whoever uses the Internet, telephone or any other information and communication technology to contact a person under the age of sixteen years and proposes to meet that person in order to commit any of the criminal offences described in Articles 183 and 189, as long as such a solicitation is accompanied by material deeds aimed at such an approaching, shall be punished with a prison sentence of one to three years or a fine of twelve to twenty-four months, without prejudice to the relevant penalties for the criminal offences actually committed. The penalties shall be imposed in the upper half when the approach is obtained by coercion, intimidation or deceit.

2. Whoever uses the Internet, telephone or any other information and communication technology to contact a person under the age of sixteen years and carries out acts aimed at luring that person into sending him pornographic material or showing him pornographic images in which a minor is displayed or appears, shall be punished with a prison sentence of six months to two years.

BUDAPEST CONVENTION ARTICLES WITH A FACILITATING CONNECTION TO CYBERVIOLENCE

5.5.19.4 ARTICLE 2 illegal access to a victim' s system is common in cyberthreats, cyberstalking, sextortion, and other forms of privacy violations amounting to cyberviolence.

Article 197 bis paragraph 1 Spanish Penal Code:
Whoever, by any means or procedure and in breach of the security measures established to prevent it, and without being duly authorised, accesses or provides another with access to a computer system or part thereof, or who remains within it against the will of whoever has the lawful right to exclude him, shall be punished with a prison sentence of six months to two years.

Article 197.6 paragraph 7 Spanish Penal Code (Sexting)
7. Whoever, without the authorisation of the affected party, discloses, communicates or reveals images or audiovisual recordings to third parties, obtained with the affected party's consent in a private residence or at any other location out of the sight of third parties, if said disclosure seriously damages the personal privacy of the individual, shall be punished with a prison sentence of three months to one year or a fine of six to twelve months.
The penalty shall be imposed in the upper half of the sentencing range if the deeds were committed by the spouse or the person who is or has been bound to him by a similar emotional relation, even without cohabitation, the victim were a minor or a person with disabilities requiring special protection, or the deeds were committed for profit.

Article 172 ter Spanish Penal Code (Stalking and Cyberstalking)
1. Whoever harasses a person by insistently and repeatedly engaging in any of the following behaviours, without being legitimately authorised, and, in this manner, severely alters his daily life, shall be punished with a prison sentence of three months to two years or a fine of six to twenty-four months:
1. Monitoring, pursuing or seeking his physical proximity;
2. Establishing or trying to establish contact *with him through any method of communication*, or through third parties;
3. *Through the inappropriate use of his personal data to purchase products or merchandise, or to sign up to services,* or having third parties contact him;
4. Infringing upon his freedom or his property, or upon the freedom or property of another person who is close to him.
In the case of an especially vulnerable individual due to his age, illness or situation, a prison sentence of six months to two years shall be imposed.
2. If the offended person is one of those referred to in Section 2 of Article 173, a prison sentence of one to two years shall be imposed, or community service from sixty to one hundred and twenty days. In this case, the formal complaint referred to in Section 4 of this Article shall not be required.
3. The punishments outlined in this Article shall be imposed without prejudice to those that could correspond to the criminal offences to which the acts of physical or psychological violence could have given rise to.
4. An individual may only be prosecuted for the deeds described in this Article if the injured party or his legal representative files a formal complaint

5.5.19.5 ARTICLE 3 – Illegal interception

Article 197 bis paragraph 2 Spanish Penal Code

2. Whoever, by using technical devices or tools, and without being duly authorised, intercepts non-public computer-based data transfer to, from or within an information system, including the electromagnetic emissions thereof, shall be punished with a prison sentence of three months to two years or a fine of three to twelve months.

5.5.19.6 ARTICLE 4 – Data interference

Article 264 Spanish Penal Code

1.Whoever, by any means, without authorisation and in a serious way, were to erase, damage, deteriorate, alter, suppress, or make data, computer programs or electronic documents pertaining to others inaccessible, if the result produced is serious, shall be punished with a prison sentence of six months to three years.

2. A prison sentence of two to five years and a fine of one to ten times the amount of damage caused shall be imposed, when any of the following circumstances concurs in the conduct described:

1. If committed within the setting of a criminal organisation;

2. If they cause particularly serious damage or damage that affects a large number of computer systems.

3. If the deed causes severe detriment to the operation of essential public services or the provision of goods of primary necessity;

4. If the deeds have affected the computer system of a critical infrastructure or have created a situation of serious danger for the security of the State, of the European Union or of a Member State of the European Union. To this effect, critical infrastructure shall be construed as an element, system or part thereof that is essential for the maintenance of the vital functions of society, health, security, protection and economic and social welfare of the population, the disruption or destruction whereof would have a significant impact as a result of the failure to maintain such functions;

5. The criminal offence has been committed by using any of the means outlined in Article 264 ter.

If the deeds have produced extremely serious effects the higher degree penalty shall be imposed.

3. The penalties imposed shall be higher by one degree to those respectively stated in the previous Sections when the deeds are committed through the unauthorised use of the personal data of another person to provide access to the computer system or to secure the trust of a third party.

5.5.19.7 ARTICLE 5 - System interference

Article 264 bis Spanish Penal Code

1. Whoever, without authorisation and in a serious way, hinders or interrupts the operation of a computer system pertaining to another in any of the following manners shall be punished with a prison sentence of six months to three years:

a) By engaging in any of the conducts outlined in the preceding Article;

b) By introducing or transferring data, or;

c) By destroying, damaging, disabling, eliminating or substituting a computer or telematic system or of electronic data storage.

If the deeds were to significantly hinder the normal activity of a company, business or Public Administration, the penalty shall be imposed in its upper half and up to the highest degree.

2. If any of the circumstances outlined in Section 2 of the preceding Article concurs in the case of the deeds foreseen in the previous Section, a prison sentence of three to eight years and a fine of three to ten times the amount of the damage caused shall be imposed.

3. The penalties imposed shall be higher by one degree to those respectively stated in the previous Sections when the deeds are committed through the unauthorised use of the personal details of another person to provide access to the computer system or to secure the trust of a third party.

5.5.19.8 ARTICLE 6 - Misuse of devices.

Article 197 ter Spanish Penal Code
Whoever, without being duly authorised, produces, acquires for use, imports or, in any way, with the intention of facilitating the perpetration of any of the criminal offences outlined in Sections 1 and 2 of Article 197 or Article 197 bis, provides third parties with:
a) A computer programme, designed or adapted primarily for the purpose of committing such criminal offences, or;

b) A computer password, an access code or similar data enabling access to all or part of an information system, shall be punished with a prison sentence of six months to two years or a fine of three to eighteen months.

Article 264 ter Spanish Penal Code
Whoever, without being duly authorised, produces, acquires for use, imports or, in any way, with the intention of facilitating the perpetration of any of the criminal offences outlined in the two preceding Articles, provides third parties with:
a) A computer program, designed or adapted primarily for the purpose of committing any of the criminal offences outlined in the two preceding Articles, or;
b) A computer password, an access code or similar data enabling access to all or part of an information system, shall be punished with a prison sentence of six months to two years or a fine of three to eighteen months.

5.5.20 United States of America

PART 1: Extracts of Domestic Legal Provisions
Representative federal statutes regarding relevant cyberviolence issues are provided below. Many states have also enacted laws criminalizing various forms of cyberbullying, revenge pornography, and the like.

1. Cyberstalking, 18 United States Code Section 2261A(2)

Whoever --
(2) with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that—
(A) places that person in reasonable fear of the death of or serious bodily injury to a person described in clause (i), (ii), or (iii) of paragraph (1)(A); or
(B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of paragraph (1)(A),
shall be punished as provided in section 2261(b) of this title.
2261(b): Penalties.—A person who violates . . . section 2261A shall be fined under this title, imprisoned—
(1) for life or any term of years, if death of the victim results;
(2) for not more than 20 years if permanent disfigurement or life threatening bodily injury to the victim results;
(3) for not more than 10 years, if serious bodily injury to the victim results or if the offender uses a dangerous weapon during the offense;
(4) as provided for the applicable conduct under chapter 109A if the offense would constitute an offense under chapter 109A (without regard to whether the offense was committed in the special maritime and territorial jurisdiction of the United States or in a Federal prison); and
(5) for not more than 5 years, in any other case,
or both fined and imprisoned.

(6) Whoever commits the crime of stalking in violation of a temporary or permanent civil or criminal injunction, restraining order, no-contact order, or other order described in section 2266 of title 18, United States Code, shall be punished by imprisonment for not less than 1 year.

2. Interstate Threats, 18 United States Code Section 875(c) & (d)

(c) Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.
(d) Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both.

3. Extortion Involving Computers, 18 United States Code Section 1030(a)(7)

Whoever –
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—
(A) threat to cause damage to a protected computer;
(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or
(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;
shall be punished as provided in subsection (c) of this section
Punishment:
(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),[4] or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

4. Obscene or Harassing Phone Calls, 47 United States Code Section 223(C), (D), & (E):

Whoever –
(C) makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to abuse, threaten, or harass any specific person;
(D) makes or causes the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number; or
(E) makes repeated telephone calls or repeatedly initiates communication with a telecommunications device, during which conversation or communication ensues, solely to harass any specific person; or
(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,
shall be fined under title 18 or imprisoned not more than two years, or both.

Part 2: Links to Domestic Policies, Strategies, or Responses to Online Violence
https://www.justice.gov/usao/file/851856/download

5.6 Examples of cases

5.6.1 Andorra

1. Country: Principality of Andorra	
2. Name of the Court: High Court of Justice of the Principality of Andorra	
3. Date of the decision: 15/09/2011	**4. Case number: TC-051-1/08**
5. Parties to the case: J.O.P vs H.M.R	
6. Decision available on the Internet? ☒Yes ☐ No http://www.justicia.ad/ca/jurisprudencia/4787.html?view=sentencia&format=pdf	
7. Topics /Key terms: infringing security measures	
8. Summary of the facts (as reflected in the decision): H.M.R. was an employee of a private security company. He felt in love with a colleague who was involved in an extramarital relationship. From February to May 2008, H.M.R. send numerous sms (11 each day aprox.) informing J.O.P. about her husband extramarital relation. Those sms were written in a menacing tone. Later on, he took advantage of working in a private security company to install illegally and in several occasions a camera to video record and take pictures of the above mentioned extramarital relation. Moreover H.M.R. send anonymously these images to J.O.P. to menace, extort and finally causing her an anxiety and depression disorder. H.M.R. was found guilty of infringement of the right to respect for private life for using a video illegally and was sentenced to three years of prison.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: Legislative decree of 29-4-2015, publishing the revised organic Law 9/2005 of 21 February, of the Criminal Code. (https://www.bopa.ad/bopa/027038/Documents/la27038001.pdf) Article 183 Escoltes il·legals i conductes afins El qui per vulnerar la intimitat d'un altre sense el seu consentiment intercepti les seves telecomunicacions o utilitzi artificis tècnics d'escolta, consulta electrònica, transmissió, gravació o reproducció del so o de la imatge, o de qualsevol altre senyal de comunicació, ha de ser castigat amb pena de presó d'un a quatre anys. La temptativa és punible.[121]	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☒ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐	

[121] Informal translation: Article 183 Illegal listening and related conduct. Whoever, in order to violate the privacy of another without their consent, intercept their telecommunications or use technical devices for listening, electronic consultation, transmission, recording or reproduction of the sound or image, or of any other communication signal, must be punished with a prison sentence of one to four years. The attempt is punishable.

Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s):

1. Country: Principality of Andorra	
2. Name of the Court: High Court of Justice of the Principality of Andorra	
3. Date of the decision: 28/07/2015	**4. Case number: 4400026/2010**
5. Parties to the case: Andorra vs J.P.P.	
6. Decision available on the Internet? ☒Yes ☐ No http://www.justicia.ad/ca/jurisprudencia/8551.html?view=sentencia&format=pdf	
7. Topics /Key terms:	
8. Summary of the facts (as reflected in the decision): J.P.P., police officer at the Andorra's Police Department, took advantage of his condition and privileges as member of the Police Department to access to several electronic databases. Those databases contain private personal data and he looked for specific information with the aim to give to his close friend T.P.C. details about his ex-wife S.L.Z. This information was used by T.P C. for spying her movements within Andorra and also for controlling anything related to her new partner J.S.B. J.P P. gave details about when S.L.Z. or J.S.B were entering or leaving the country, number plate of his vehicle, work schedule, telephone numbers and personal address, among other personal information. With this information provided by J. P. P., T.P.C send several menacing letters and messages to S. L. Z. J. P. P. was found guilty of and offence for the disclosure of confidential information and was conditionally sentenced to two years of prison and excluded of the Police Service for four years.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: Legislative decree of 29-4-2015, publishing the revised organic Law 9/2005 of 21 February, of the Criminal Code. (https://www.bopa.ad/bopa/027038/Documents/la27038001.pdf) Article 377 Revelació de secrets 1. L'autoritat o el funcionari que reveli secrets o informacions que no afectin la intimitat d'una persona, dels quals tingui coneixement per raó del seu càrrec i que no hagin de ser divulgats, ha de ser castigat amb pena d'inhabilitació per a l'exercici de càrrec públic fins a tres anys. 2. El particular que reveli secrets o informacions de les descrites a l'apartat anterior ha de ser castigat amb pena de multa fins a 6.000 euros. 3. Si la revelació a la qual es refereixen els apartats anteriors afecta la intimitat d'una persona la pena ha de ser de presó de tres mesos a tres anys i inhabilitació per a l'exercici de càrrec públic fins a cinc anys	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☒ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐	

Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s):

1. Country: Principality of Andorra	
2. Name of the Court: High Court of Justice of the Principality of Andorra	
3. Date of the decision: 30/03/2015	**4. Case number: 6000007/2014**
5. Parties to the case: Andorra vs. J.L.C.S	
6. Decision available on the Internet? ☒Yes ☐ No First instance sentence. http://www.justicia.ad/ca/jurisprudencia/8237.html?view=sentencia&format=pdf Appeal. http://www.justicia.ad/ca/jurisprudencia/8685.html?view=sentencia&format=pdf	
7. Topics /Key terms: Child pornography	
8. Summary of the facts (as reflected in the decision): The defendant J.L.C.S., a Spanish citizen, was accused of distribution and deliberate possession of pornographic images showing young children practicing explicit sexual activities using computerized means. In particular, he shared at least 6 computer files with other users, all of these files containing pornographic material. The Tribunal sentenced him to two years of imprisonment by committing an offence of using minors for pornographic purpose. The defendant filed an appeal against the sentence, but the court of appeal did not find grounds to reverse the lower court's sentence, so that the sentence was upheld in all its aspects.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: Art. 155.2 of the Legislative decree of 29-4-2015, publishing the revised organic Law 9/2005 of 21 February, of the Criminal Code. https://www.bopa.ad/bopa/027038/Documents/la27038001.pdf Capítol quart. Delictes relatius a la pornografia i les conductes de provocació sexual Article 155. Utilització de menors i incapaços per a la pornografía. 2. Qui recluti, utilitzi un menor o un incapaç amb finalitats pornogràfiques o exhibicionistes o n'afavoreixi la participació, i qui produeixi, adquireixi, vengui, importi, exporti, distribueixi, difongui, cedeixi o exhibeixi per qualsevol mitjà material pornogràfic en el qual apareguin imatges de menors dedicats a activitats sexuals explícites, reals o amb aparença de realitat, o qualsevol altra representació de les parts sexuals d'un menor amb finalitats primordialment sexuals, ha de ser castigat amb pena de presó d'un a quatre anys. La temptativa és punible. La proposició per mitjà de les tecnologies de la informació i la comunicació d'una trobada amb un menor de catorze anys, amb la finalitat de cometre la infracció descrita al paràgraf anterior, es considera temptativa si la proposició ha estat seguida d'actes materials que condueixin a la dita trobada.[122]	

[122] Informal translation: Fourth chapter Crimes related to pornography and behavior of sexual provocation.

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):

1. Country: Principality of Andorra

2. Name of the Court: High Court of Justice of the Principality of Andorra

3. Date of the decision: 05/09/2015	**4. Case number: TC-119-4/12**

5. Parties to the case: Andorra vs. R.R.G.

6. Decision available on the Internet? ☒Yes ☐ No
http://www.justicia.ad/ca/jurisprudencia/7211.html?view=sentencia&format=pdf

7. Topics /Key terms:
Child pornography

8. Summary of the facts (as reflected in the decision):
R.R.G. was accused of possession of pornographic images showing young children practicing explicit sexual activities using computerized means for at least 5 years. The monitoring of the defendant was possible by an alert received by Interpol Germany.
According to the investigation followed then by the Police of Andorra, the defendant had at least 1.360 computer files containing pornographic material.

The Tribunal sentenced him to two years of imprisonment by committing an offence of using minors for pornographic purpose.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
Art. 155.2 and art. 155.3 of the Legislative decree of 29-4-2015, publishing the revised organic Law 9/2005 of 21 February, of the Criminal Code.

Article 155. Use of minors and disabled for pornography. 2. Whoever recruits, uses a minor or a disabled person for pornographic or exhibition purposes or favours the participation, and who produces, acquires, sells, imports, exports, distributes, disseminates, cede or exhibits by any means pornographic material in which images of minors devoted to explicit sexual activities, real or with appearance of reality, or any other representation of the sexual parts of a child with primarily sexual purposes, must be punished with a prison sentence of one to four years. The attempt is punishable. The proposal through information and communication technologies of a meeting with a minor of fourteen years, in order to commit the infraction described in the previous paragraph, is considered an attempt if the proposal has been followed by material acts that lead to this encounter.

https://www.bopa.ad/bopa/027038/Documents/la27038001.pdf

Capítol quart. Delictes relatius a la pornografia i les conductes de provocació sexual

Article 155. Utilització de menors i incapaços per a la pornografía. 2. Qui recluti, utilitzi un menor o un incapaç amb finalitats pornogràfiques o exhibicionistes o n'afavoreixi la participació, i qui produeixi, adquireixi, vengui, importi, exporti, distribueixi, difongui, cedeixi o exhibeixi per qualsevol mitjà material pornogràfic en el qual apareguin imatges de menors dedicats a activitats sexuals explícites, reals o amb aparença de realitat, o qualsevol altra representació de les parts sexuals d'un menor amb finalitats primordialment sexuals, ha de ser castigat amb pena de presó d'un a quatre anys. La temptativa és punible. La proposició per mitjà de les tecnologies de la informació i la comunicació d'una trobada amb un menor de catorze anys, amb la finalitat de cometre la infracció descrita al paràgraf anterior, es considera temptativa si la proposició ha estat seguida d'actes materials que condueixin a la dita trobada. 3. Qui ofereixi, posseeixi, procuri per a ell o per a un altre, o accedeixi a través de qualsevol tecnologia de la comunicació o la informació a material pornogràfic en el qual apareguin imatges de menors dedicats a activitats sexuals explícites, reals o amb aparença de realitat, o qualsevol altra representació de les parts sexuals d'un menor amb finalitats primordialment sexuals, ha de ser castigat amb pena de presó d'una durada màxima de dos anys. La temptativa és punible.

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):

5.6.2 Austria

1. Country: AUSTRIA

2. Name of the Court:
REGIONAL COURT IN CRIMINAL MATTERS VIENNA

3. Date of the decision:	**4. Case number:**
15.2.2017	**Cannot be disclosed due to data protection**

5. Parties to the case:
Cannot be disclosed due to data protection

6. Decision available on the Internet? ☐Yes ☒ No

7. Topics /Key terms:
e.g. cyberbullying; cyberviolence, grooming, sexting, social networks
cyberviolence

8. Summary of the facts (as reflected in the decision): [no more than 200 words]
A group of six juveniles aged between 15 and 21 forced a victim to come with them to a garage of a large shopping mall in Vienna. There five of them started hitting the victim in the face and head (22 times) which was filmed by the sixth member of the group of offenders. The victim suffered

among several bruises two mandibular fractures and had to undergo surgery.
In first place the video was shared via Whatsapp with a group of other persons and afterwards published on Facebook where it was published on Facebook where more than one million users viewed the video and commented on it.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
The whole group of offenders was found guilty for serious assault in accordance with Sec 84 paras 4 and 5 subpara 2:
§ 84. (1) Any person who does bodily harm thus negligently causing damage to health for a period of more than 24 days or an incapacity to work or serious physical injury or damage to health is liable to imprisonment for up to three years.
(2) The same penalty applies to any person who assaults (§ 83 para. 1 or para. 2) a Government official, a witness or expert witness during or because of the execution of that person's duties.
(3) The same penalty applies if the person has committed three separate offences (§ 83 para. 1 or para. 2) unprovoked and by using substantial violence.
(4) Any person who does physical injury or damage to the health of another thus causing, even if negligently, serious physical injury or damage to health (para. 1) is liable to imprisonment for six months to five years.
(5) The same penalty applies to any person who commits an assault (§ 83 para. 1 or para. 2)
1. in a manner involving risk of death,
2. in concert with at least two persons, or
3. by inflicting exceptional pain.

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s): N/A

5.6.3 Chile

1. Country:
Chile

2. Name of the Court:
7th Investigative Criminal Court of Santiago (7o. Juzgado de Garantía de Santiago)

3. Date of the decision:	**4. Case number:**
October 28th, 2013	1201164510-9

5. Parties to the case: Mauricio Coronado Mesa

6. Decision available on the Internet? ☒Yes ☐ No
If yes, please provide a working link

7. Topics /Key terms:
Grooming, social networks

8. Summary of the facts (as reflected in the decision):
Through Facebook, the defendant sent to several girls (less than 14 years) links to or images of child pornography or similar sexual content.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
Art. 366 quáter of the Criminal Code (http://bcn.cl/1uvd5).
Art. 374 bis of the Criminal Code.

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
Not applicable.

1. Country:
Chile

2. Name of the Court:
Investigative Criminal Court of Chiguyante

3. Date of the decision:	**4. Case number:**
December 4th, 2014	1410008228-5

5. Parties to the case: Manuel Emilio López Orellana

6. Decision available on the Internet? ☒**Yes** ☐ **No**
If yes, please provide a working link
If not, if possible, please provide as a word or PDF file

7. Topics /Key terms:
Grooming, social networks

8. Summary of the facts (as reflected in the decision):
The defendant caused several young girls to send him photos of the latters of a sexual nature and kept images of child pornography.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
Art. 366 quáter of the Criminal Code (http://bcn.cl/1uvd5).
Art. 374 bis of the Criminal Code.

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
Not applicable.

1. Country:

Chile
2. Name of the Court: Court of Appeals of Chillán, Criminal Trial Court of Chillán.

3. Date of the decision:	**4. Case number:**
September 29th, 2015	1300368477-0

5. Parties to the case: Manuel Antonio Ayavire Ferre
6. Decision available on the Internet? ☒**Yes** ☐ **No** If yes, please provide a working link
7. Topics /Key terms: Cyberbullying; grooming, social networks
8. Summary of the facts (as reflected in the decision): The defendant contacts an underage girl in Uruguay and, misrepresenting his age, obtains from the victim photos wearing just underwear, obtaining later photos of sexual content under threats of releasing the first ones.
9. Summary of applicable legal provision(s) and of reasoning of the Court: Art. 366 quáter of the Criminal Code.
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☒ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s): Not applicable.

1. Country: Chile
2. Name of the Court: 11th Criminal Investigative Court of Santiago

3. Date of the decision:	**4. Case number:**
January 12th, 2015	1400609227-7

5. Parties to the case: Manuel Andres Torres Castro
6. Decision available on the Internet? ☒**Yes** ☐ **No** If yes, please provide a working link
7. Topics /Key terms: Grooming, social networks
8. Summary of the facts (as reflected in the decision): The defendant, under threats of releasing private photos, obtained nude photos of girls of less than 14 years of age and kept them stored in his computer.
9. Summary of applicable legal provision(s) and of reasoning of the Court: Art. 366 quáter of the Criminal Code.
10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
Not applicable.

1. Country:
Chile

2. Name of the Court:
Criminal Trial Court of Curicó

3. Date of the decision:	**4. Case number:**
February 3rd, 2017	1501025760-0

5. Parties to the case: [
Juan Pablo Parra Trujillo

6. Decision available on the Internet? ☒Yes ☐ No
If yes, please provide a working link

7. Topics /Key terms:
Grooming, social networks

8. Summary of the facts (as reflected in the decision):
The defendant sent photos of his genitalia to the 13-years-old victim and requested photos of her breast through Whatsapp, not achieving his purpose, as the victim did not send requested images.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
Art. 366 quáter of the Criminal Code.

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
Not applicable.

1. Country:
Chile

2. Name of the Court:
Criminal Trial Court of Viña del Mar

3. Date of the decision:	**4. Case number:**
March 1st, 2016	1400681649-6

5. Parties to the case:

Rubén Andrés Salinas Valero
6. Decision available on the Internet? ☒Yes ☐ No If yes, please provide a working link
7. Topics /Key terms: Grooming, social networks
8. Summary of the facts (as reflected in the decision): The defendant, a former teacher of the victim, perform acts of sexual nature before the underage victim consisting in messages through Facebook through which he sent photos of his genitalia, he ask her to engage in sexual relations with him and he requested photos of her genitalia.
9. Summary of applicable legal provision(s) and of reasoning of the Court: Art. 366 quáter of the Criminal Code
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☒ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s): Not applicable.

5.6.4 France

1. Country: France
2. Topics /Key terms: Provocation to commit suicide with the aggravating circumstance that the victim is a minor, Distribution of messages inciting minors to commit suicide
3. Summary of the facts (as reflected in the decision): While surfing on the Blue Whale Challenge's Facebook account, the victim met a "step-father" and started chatting with him via Messenger. Having some personal issues with her family and friends and feeling quite disoriented in her day-to-day life, she decides to start the first test of the challenge i.e scarifying herself, listening to sad music... Her mother, discovering what her daughter was up to, was able to make her speak and stop the challenge (after the 4th test). Despite technical investigation, the step-father wasn't identified; the case is now closed.
4. Summary of applicable legal provision(s) : 223-13 and 227-24 Penal Code
5. Possibly relevant provisions of the Budapest Convention: none Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐

Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

1. Country: France

2. Topics /Key terms:
Sexual Harassment

3. Summary of the facts (as reflected in the decision):

Using his position as a teacher, the offender started sending text messages to various of his students (under 15 years old) in order to get closer and start personal interaction sometimes based on sexual perspective.

4. Summary of applicable legal provision(s) : Art 222-33 Penal Code

5. Possibly relevant provisions of the Budapest Convention: none

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

1. Country: France

2. Topics /Key terms:
Sexual extortion of sexual material.

3. Summary of the facts (as reflected in the decision):

Using an online dating application, the victim met the offender and started discussing and sending nude pictures as requested on an exchange perspective. Seeing that the offender is not sending anything, the victim, young adult, decided to stop chatting and moved away. Unfortunately, the offender didn't hear the thing this way and asked for more nude pictures using threat to reveal and publish online the previous pictures sent. In order to stop the threat, the offender asked also for 300 euros to be deposit in a famous square of his town. After a couple of new pictures, the victim went to the police to report the extortion. Under police surveillance, the victim agreed to deposit the envelope with the money at the accorded destination. The offender was arrested while retrieving the envelope and convinced of extortion based on a technical analysis of his telephone.

4. Summary of applicable legal provision(s) : Art 312-1 Penal Code

5. Possibly relevant provisions of the Budapest Convention: none

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

1. Country: France

2. Topics /Key terms:

financial extortion based on sexual exchange (sextortion)

3. Summary of the facts (as reflected in the decision):

Using an online dating application, the victim met a woman and started discussing via Skype. Within few minutes, the woman asked about explicit sexual discussion and online sex, showing her breast then using a sex toy asking to see the victim naked. Once the victim has agreed and shown him naked online, he received some messages saying that if he was willing to send some money, the video taken of his strip-tease won't be released on line and to his Facebook's friends.
The victim shut down his computer, cancelled his account on the dating site and didn't respond to any messages sent by the offender. However, he received some email from pretended YouTube company asking for some money in order to delete the video which was contrary to the YouTube policy and could take the victim to court for online exhibitionism. The victim went to the police to complain about this extortion attempt.
The offender was not identified, located in a foreign country.

4. Summary of applicable legal provision(s) : Art 312-1 Penal Code

5. Possibly relevant provisions of the Budapest Convention: none

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

1. Country: France

2. Topics /Key terms:
Slander

3. Summary of the facts (as reflected in the decision):
The offender sends thousands email to the victim, civil servant, in which he questioned its impartiality and effectiveness at work.

4. Summary of applicable legal provision(s) :

5. Possibly relevant provisions of the Budapest Convention: none

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

1. Country: France

2. Topics /Key terms:
System interference

3. Summary of the facts (as reflected in the decision):
Various Police Stations call center has been connected through conference call where one offender insulted the police officers. One of the phone numbers used was from UK (spoofed number).

4. Summary of applicable legal provision(s) : Article 323-1, Article 323-2 Penal Code

5. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference X
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

1. Country: France

2. Topics /Key terms:
System interference

3. Summary of the facts (as reflected in the decision):
Emergency Call Center was victim of a DDOS attack during 15 min (Telephone DOS) that conducted the call center to an interruption of service. Investigations are still ongoing but action might be voluntary.

So far, no evidence regarding the use of a botnet or dedicated online service/app used.

4. Summary of applicable legal provision(s) : Article 323-1, Article 323-2 Penal Code

5. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference X
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

1. Country: France

2. Topics /Key terms:
Swatting / spoofing / false statement

3. Summary of the facts (as reflected in the decision): The offender called the police station and declared that he has just killed his wife, is armed and will kill anyone who might come to his house. SWAT teams sent to the address broke and entered the house in order to arrest the individuals present. Unfortunately, the man arrested was a victim of a "joke" by someone who spoofed his phone number in order to call the police and report the fake murder.
Investigations are still ongoing.

4. Summary of applicable legal provision(s) :

5. Possibly relevant provisions of the Budapest Convention: none

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

1. Country: France

2. Topics /Key terms:
Hate speech

3. Summary of the facts (as reflected in the decision):
A suspected far-right extremist has been charged with plotting to kill French President Emmanuel Macron at the Bastille Day parade later this month.
The 23-year-old was arrested in a Paris suburb after police was alerted by users of a videogame chat room where he allegedly said he wanted to buy a gun and wanted to attack minorities, such as muslims, jews, blacks and homosexuals. The investigations provided on his belongings confirmed the plot and upstream research on its victims.

4. Summary of applicable legal provision(s) :

5. Possibly relevant provisions of the Budapest Convention: none

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

1. Country: France

2. Name of the Court: Cour d'Appel de Paris

3. Date of the decision:	**4. Case number: N/A**
10 oct. 2014	

5. Parties to the case:
N/A

6. Decision available on the Internet? ☐Yes ☒ No

7. Topics /Key terms:
identity theft

8. Summary of the facts (as reflected in the decision):
the defendant was sentenced to 10 months imprisonment and € 30,000 for creating false Facebook profiles and false ads on dating sites in order to harm the director of the company with who he had a commercial dispute

9. Summary of applicable legal provision(s) and of reasoning of the Court:
Identity theft (226-4-1 CP)

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s): N/A

1. Country: France	
2. Name of the Court: Cour d'Appel de Paris	
3. Date of the decision: 13 avril 2016	**4. Case number:** ***Affaire n°10183000010***
5. Parties to the case: Mme X. / Ministère Public, iVentures Consulting, et autres	
6. Decision available on the Internet? ☒**Yes** ☐ **No** https://www.legalis.net/jurisprudences/cour-dappel-de-paris-arret-du-13-avril-2016/	
7. Topics /Key terms: cyberbullying; cyberviolence, social networks	
8. Summary of the facts (as reflected in the decision): A young woman, out of vengeance, has used all the technological means at her disposal to insult and threaten her ex-lover and ex-cohabitant. The defendant has used the identity of the first victim and created a dozen profiles, on several social networks as well as Facebook pages (photographs in support), intended to discredit him in his professional environment. As for the second, she had been harassing him since their break with hateful messages (849 SMS of insults and threats over 10 months).	
9. Summary of applicable legal provision(s) and of reasoning of the Court: Several criminal qualifications were used: impersonation of a third party's digital identity, harassment by a concubine (Penal C., art. 222-33-2-1), impairment of the representation of the person (Penal C. , 226-8), repetitive mailings of malicious messages, threats of violence. The defendant was sentenced for two years imprisonment, one of which is suspended.	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐	
11. Useful online link(s): N/A	

5.6.5 Israel

1. Country: Israel	
2. Name of the Court:	
3. Date of the decision:	**4. Case number:**
5. Parties to the case:	
6. Decision available on the Internet? ☐**Yes** ☒ **No**	
7. Topics /Key terms: Threats, Email, Harassment	
8. Summary of the facts (as reflected in the decision):	

The suspect is a known, serial, harasser. The Israeli Police is investigating 15 different cases of occasions when the suspect used to threaten Israeli public officials (including the PM).
The suspect left Israel and presumably lives in England or Canada.

9. Summary of applicable legal provision(s) and of reasoning of the Court:

Article 192 to the Israeli Penal Code (1977) – Threatening

10. Possibly relevant provisions of the Budapest Convention:
Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☒
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s): N/A

1. Country: Israel

2. Name of the Court: The district court in Haifa

3. Date of the decision:	**4. Case number:**

5. Parties to the case:

6. Decision available on the Internet? ☐Yes ☒ No

7. Topics /Key terms:
cyberbullying, cyberviolence, grooming, sexting, social networks

8. Summary of the facts (as reflected in the decision):
The 16 years old teenager impersonated a teenage girl using Skype, and corresponded with the victims using a few fake accounts.
As part of the correspondence, that defendant forced the 14 years old victim to expose his genitals and to rape his younger, 10 years old, brother.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
Article 368C to the Israeli Penal Code (1977) – abuse of minors
Article 347 to the Israeli Penal Code (1977) - Sodomy of a minor
Article 428 to the Israeli Penal Code (1977) – extortion

10. Possibly relevant provisions of the Budapest Convention:
Article 2 – Illegal access ☐
Article 3 – Illegal interception ☒
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☒
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐

Article 9 – Offences related to child pornography ☒ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s):

1. Country: Israel	
2. Name of the Court: Nazareth District Court	
3. Date of the decision:	**4. Case number:**
5. Parties to the case:	
6. Decision available on the Internet? ☐Yes ☒ No	
7. Topics /Key terms: Paedophilia, Facebook, Harassment, Blackmail	
8. Summary of the facts (as reflected in the decision): The suspect was arrested after being accused of sexually harassing 20 minors. Since 2012, the suspect used fake Facebook profiles (using a picture of a young boy) in order to contact 12-13 years old girls. Between the years 2012-2016, the suspect used those profiles to send, demand and receive intimate photos of the minors. Moreover, he accessed websites containing child pornography, and saved pedophilic content on his personal computer.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: The Protection of Privacy Act (1981) – Intrusion of privacy Article 441 to the Penal Code (1977) - Impersonation The Prevention of Sexual Harassment Act (1998) - Sexual Harassment Article 214(b3) to the Penal Code (1977) – Possession of pedophilic content	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☒ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☒ Article 10 – Offences related to infringements of copyright and related rights ☐	
11. Useful online link(s):	

1. Country: Israel

2. Name of the Court: The district court in Tel-Aviv

3. Date of the decision:	**4. Case number:** **1999/17**

5. Parties to the case: The State of Israel v. John Doe (three defendants)

6. Decision available on the Internet? ☒**Yes** ☒ **No**

One of the Supreme Court's decisions in the arrest process of the defendants - https://www.nevo.co.il/psika_html/elyon/17019990-o01.htm

7. Topics /Key terms:
cyberviolence, social networks, incitement

8. Summary of the facts (as reflected in the decision):

The three defendants are the managers of numerous blogs and websites dedicated to defamation against civil servants, operated since 2009. The defendants have deliberately aimed specific civil servants – social workers, judges, policemen, state attorneys and more - in order to discourage them from preforming their public duties. The defendants have carried out a campaign of defamation, sexual harassment, intrusion of privacy, threatening and other offences in what has been regarded by the Israeli Supreme Court as "online terrorism".

9. Summary of applicable legal provision(s) and of reasoning of the Court:

The Prevention of Sexual Harassment Act (1998)
The Protection of Privacy Act (1981)
The Prohibition of Defamation Act (1965)
Article 255 to the Israeli Penal Code (1977) - Contempt of court
Article 192 to the Israeli Penal Code (1977) – Threatening

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☒
Article 8 – Computer related fraud ☒
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):

1. Country: Israel

2. Name of the Court:

3. Date of the decision:	**4. Case number:**

5. Parties to the case:

6. Decision available on the Internet? ☐Yes ☒ No

7. Topics /Key terms:
cyberbullying; cyberviolence, sexting, social networks

8. Summary of the facts (as reflected in the decision):

Two 13 years old minors are suspects for breaking into Snapchat accounts of 60 minors (girls) and blackmailing them after finding intimate pictures in the accounts.
As the investigation proceeded it was found out that the suspects used to contact minors (girls) from different parts of Israel, develop friendly relations with the minors and receiving intimate pictures of their victims. After receiving the pictures, they used to extort the minors into sending them more and more intimate documentation, including inserting objects to the minors' genitals.

9. Summary of applicable legal provision(s) and of reasoning of the Court:

The Protection of Privacy Act (1981) – intrusion of privacy
The Penal Code (1977) – extortion
The Computers Act (1995) – illegal access to computer material
The Prevention of Sexual Harassment Act (1998) – Sexual Harassment

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☒
Article 3 – Illegal interception ☒
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s): N/A

1. Country: Israel

2. Name of the Court: Rishon Lezion Magistrate Court

3. Date of the decision:	**4. Case number:**

5. Parties to the case:

6. Decision available on the Internet? ☐Yes ☒ No

7. Topics /Key terms:
Blackmailing, child extortion, Instagram

8. Summary of the facts (as reflected in the decision):

A 17 year old is suspect for corresponding with minors via Instagram chat. The suspect convinced

the victims to send him intimate photos of them and later blackmailed them using those photos. Information that was received from the ISPs led to the identification of the suspect and to the realization that he is connected to 10 other cases.
9. Summary of applicable legal provision(s) and of reasoning of the Court: Article 214(b) to the Israeli Penal Code (1977) – Publishing pedophilic content. The Prevention of Sexual Harassment Act (1998) – Sexual Harassment Article 428 to the Israeli Penal Code (1977) – Extortion
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☒ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☒ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s): Media publications regarding the case: http://www.maariv.co.il/news/israel/Article-583628 http://www.ynet.co.il/articles/0,7340,L-4958519,00.html

1. Country: Israel	
2. Name of the Court: The Jerusalem Court	
3. Date of the decision:	**4. Case number:**
5. Parties to the case:	
6. Decision available on the Internet? ☐Yes ☒ No	
7. Topics /Key terms: Fraud, Harassment, Shaming, Spam, Personal Information, Porn Sites, Sale Sites	
8. Summary of the facts (as reflected in the decision): The suspect, supposedly working in the field of internet advertisement, committed fraud crimes against dozens of victims. After these crimes, the victims would file a lawsuit against him or a police complaint, and then the suspect would harass them. The harassments would include publishing hurtful posts on the internet; sending spam messages in their name; publishing their phone numbers on porn sites. All of these acts led to them receiving harassing phone calls.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: Article 30 the Communications Act (1982) - Harassment using a phone	

Article 192 to the Penal Code (1977) - Threatening Article 249 to the Penal Code (1977) - Harassment of a witness Article 420 to the Penal Code (1977) – Use of a fake document Article 3 to the Computers Act (1995) – Transmitting false information using a computer
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☒ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☒ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s):

5.6.6 Japan

1. Country: Japan	
2. Name of the Court: Kyoto District Court	
3. Date of the decision: 14/02/2017	**4. Case number:** **N/A**
5. Parties to the case: A man 28 year-old (the ringleader of child sex abuse network) v a boy	
6. Decision available on the Internet? ☐Yes ☒ No	
7. Topics /Key terms: child sex abuse	
8. Summary of the facts (as reflected in the decision): The ringleader, a man aged 28, of a child sex abuse network in Kyoto, identified via INTERPOL's International Child Sexual Exploitation (ICSE) database, has been sentenced to eight years after being found guilty of charges including child prostitution and forcible indecency. Four other members of the network, men aged between 36 and 40, were convicted between October and December 2016 and handed down sentences ranging between two and five years. The abusers, including a businessman, a nursing home employee and a dancer, would approach children in amusement parks, game centers and video rental shops, or in the street. After recording their crimes, the videos would be circulated via a private network. Using the ICSE database, analysis of the child's school uniform and sound data enabled victim identification specialists around the world, working with INTERPOL's Crimes Against Children (CAC) unit, to identify Japan as the probable location. INTERPOL's CAC unit alerted Japan's National Police Agency (NPA) which, determining the crime had taken place in Kyoto, notified the Kyoto Prefectural Police (KPP). KPP immediately launched citywide investigations resulting in the arrest of his suspected abuser. Interviews with the victim triggered further enquiries, identifying and dismantling the network which was engaged in the sexual abuse of 47 boys aged between seven and 15.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: Penal Code Article 176 (Forcible Indecency)	

http://www.japaneselawtranslation.go.jp/law/detail/?id=1960&vm=04&re=01&new=1

Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child Pornography, and the Protection of Children(Amendment:Act No.74 (2011～2014)) Article 7 (3), Article 2(3)(1), Article2(3)(2), Article2(3)(3)
Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child Pornography, and the Protection of Children Article 7(4), Article 2(3)(2), Article2(3)(3)
http://www.japaneselawtranslation.go.jp/law/detail/?id=2592&vm=04&re=01&new=1

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
https://www.interpol.int/News-and-media/News/2017/N2017-017/

1. Country:
Japan

2. Name of the Court:

3. Date of the decision:	**4. Case number:**
N/A	**N/A**

5. Parties to the case:
N/A

6. Decision available on the Internet? ☐**Yes** X **No**

7. Topics /Key terms:
cyberstalking

8. Summary of the facts (as reflected in the decision):
A man 42 year-old broke into the victim's house to install in the victim's smartphone an application "Track View" that can secretly activate a recording function by remote control. Thus, he succeeded in peeping the victim's activities through the recorded video.
Aichi Prefectural Police arrested the man on June 9, 2017 on the suspicion of offering electronic data for illegal control over another person's computer and violation of Anti-Stalking Act. It's the first case in Japan of stalking via a remote monitoring application.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
N/A

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐

Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☒ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s): **N/A**

1. Country: Japan	
2. Name of the Court: **N/A**	
3. Date of the decision: **N/A**	**4. Case number:** **N/A**
5. Parties to the case: **N/A**	
6. Decision available on the Internet? ☐Yes ☒ No	
7. Topics /Key terms: child pornography	
8. Summary of the facts (as reflected in the decision): The accused uploaded child pornography on the Internet and displayed it in public for the purpose of obtaining a viewing fee from browsers.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child Pornography, and the Protection of Children_Article7(6) **http://www.japaneselawtranslation.go.jp/?re=02**	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☒ Article 10 – Offences related to infringements of copyright and related rights ☐	
11. Useful online link(s): N/A	

1. Country: Japan	
2. Name of the Court: N/A	
3. Date of the decision: **N/A**	**4. Case number:** **N/A**
5. Parties to the case: **N/A**	

6. Decision available on the Internet? ☐Yes ☒ No

7. Topics /Key terms:
sexting, cyberviolence

8. Summary of the facts (as reflected in the decision):
The accused uploaded sexual image data of an ex-girlfriend on the Internet, broke into her residence and murdered her with a knife.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child pornography, and the Protection of Children_Article7(6)
Breaking into a Residence, Display of Obscene Recording Media Containing Electromagnetic Records, Homicide: Penal code_Article130,175(1),199
http://www.japaneselawtranslation.go.jp/?re=02

Display of Obscene Recording Media Containing Electromagnetic Records (Article175(1)) was revised as follows in 2011.
A person who distributes or displays in public an obscene document, drawing, recording media containing such electromagnetic records or other objects shall be punished by imprisonment for not more than 2 years, a fine of not more than 2,500,000 yen or a petty fine, or both imprisonment and a fine. The same shall apply to anyone who distributes an obscene electromagnetic record or any other record by transmission of telecommunication.

10. Possibly relevant provisions of the Budapest Convention:
Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
N/A

1. Country:
Japan

2. Name of the Court:
N/A

3. Date of the decision:	**4. Case number:**
N/A	**N/A**

5. Parties to the case:
N/A

6. Decision available on the Internet? ☐Yes ☒ No

7. Topics /Key terms:
social networks, cyberviolence

8. Summary of the facts (as reflected in the decision):
The accused impersonated an ex-girlfriend and updated her blog which hurt her reputation.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
Defamation : Penal Code_Article230(1)
http://www.japaneselawtranslation.go.jp/?re=02

10. Possibly relevant provisions of the Budapest Convention:
Article 2 – Illegal access ☒
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
N/A

1. Country:
Japan

2. Name of the Court:
N/A

3. Date of the decision:	**4. Case number:**
N/A	**N/A**

5. Parties to the case:
N/A

6. Decision available on the Internet? ☐Yes ☒ No

7. Topics /Key terms:
social networks, revenge pornography

8. Summary of the facts (as reflected in the decision):
The accused threatened an ex-girlfriend by sending messages saying that he would upload her naked image data on the Internet, and posted her naked image data on Twitter.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
Display of Obscene Recording Media Containing Electromagnetic Records, Intimidation: Penal Code_Article175(1),222(1)
http://www.japaneselawtranslation.go.jp/?re=02

Display of Obscene Recording Media Containing Electromagnetic Records (Article175(1)) was revised as follows in 2011.
A person who distributes or displays in public an obscene document, drawing, recording media containing such electromagnetic records or other objects shall be punished by imprisonment for not more than 2 years, a fine of not more than 2,500,000 yen or a petty fine, or both imprisonment and a fine. The same shall apply to anyone who distributes an obscene electromagnetic record or any other record by transmission of telecommunication.

Act on Prevention of Damage by Provision of Private Sexual Image Records_Article3(1)
A person who provides unspecified persons or a number of persons with private sexual image records through telecommunication lines in such a way that third parties can specify the individual in that image shall be punished by imprisonment for not more than 3 years or a fine of not more than 500,000 yen.

10. Possibly relevant provisions of the Budapest Convention:
Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐

Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s): **N/A**

1. Country: Japan	
2. Name of the Court: Tokyo District Court	
3. Date of the decision: 2/4/2015	**4. Case number:** **N/A**
5. Parties to the case: **N/A**	
6. Decision available on the Internet? ☐Yes ☒ No	
7. Topics /Key terms: cyberviolence	
8. Summary of the facts (as reflected in the decision): The accused posted indiscriminate murder notice on online bulletin board by using computer program having remotely control function.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: Forcible Obstruction of Business of Penal Code_Article234 **http://www.japaneselawtranslation.go.jp/?re=02**	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐	
11. Useful online link(s): **N/A**	

5.6.7 Latvia

1. Country: Latvia	
2. Name of the Court: Criminal case division/ Criminal matters collegium of Riga Regional Court	
3. Date of the decision: 28.04.2015	**4. Case number:** 12010000313
5. Parties to the case: Anonymized decision. Plaintiff – person E, defendant – person C	
6. Decision available on the Internet? ☒Yes ☐ No	

https://www.tiesas.lv/nolemumi/pdf/226336.pdf
7. Topics /Key terms: Unlawful access to data processing systems Unlawful access to the data Violating the confidentiality of correspondence and information to be transmitted over telecommunications networks
8. Summary of the facts (as reflected in the decision): At unresolved time, but not later than 29 of September 2012 *person C* while staying in her place of residence in Riga, using a computer previously used by her ex-husband - *person E*, without his admission, being aware of unlawful nature of her actions, deliberately accessed *person E* e-mail account by using saved in browser memory password. After, aware that she violates other person's privacy, *person C* read *person E* correspondence and printed it out. Later on, *person C* used data, which had been illegally obtained, as evidence in the Civil Matters Collegium of Riga Regional Court in application for maintenance payment from *person E*.
9. Summary of applicable legal provision(s) and of reasoning of the Court: The Criminal Law: http://vvc.gov.lv/image/catalog/dokumenti/The%20Criminal%20Law.docx European Convention of Human Rights: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Convention_ENG.pdf The Constitution of the Republic of Latvia : http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/Constitution.doc Protection of the Rights of the Child Law: http://www.vvc.gov.lv/export/sites/default/docs/LRTA/Likumi/ Protection_of_the_Rights_of_the_Child.doc **Reasoning of the Court:** http://at.gov.lv/files/uploads/files/archive/department2/2006/a/kd130206-1.doc http://at.gov.lv/files/uploads/files/archive/department2/2014/SKK-417-2014.doc
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☒ Article 3 – Illegal interception ☒ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s): N/A

5.6.8 Mauritius

1. Country: Mauritius	
2. Name of the Court: Intermediate Court	
3. Date of the decision: 17 September 2017	**4. Case number: CN 1142/13**
5. Parties to the case: Police v/s Jugduth Seegum	
6. Decision available on the Internet? ☒Yes ☐ No https://supremecourt.govmu.org/Search/Pages/JudgmentSearchResult.aspx?k="seegum"	
7. Topics /Key terms: Information and communication service, causing annoyance, intention, degrading and humiliating	
8. Summary of the facts (as reflected in the decision):	

Accused posted derogatory comments on Facebook forum which was initially created for 'pedagogical discussion' and which was followed by several comments and likes. Complainant feeling aggrieved reported the matter to police. The two main issue to be thrashed out were (i) annoyance and (II) intention.

9. Summary of applicable legal provision(s) and of reasoning of the Court:

Information and Communication Technologies Act 2001

Section 46(h) (ii) of the ICTA reads:
"Any person who…
(h) uses an information and communication service, including telecommunication service, -
(ii) for the purpose of causing annoyance, inconvenience or needless anxiety to any person;
shall commit an offence."

Annoyance was found proved through the testimony of the complainant who explained that she felt belittled, humiliated and affected by the comments which affected her personal life vis a vis her husband and her family. Also the comments had impediments on her role as a trade unionist.

Intention for the purpose of causing annoyance was found proved since none of the posts comments and likes were of a pedagogical nature.

Accused was found guilty on the charges preferred and was fined **Rs 45,000**.

https://supremecourt.govmu.org/Search/Pages/LegislationSearchResult.aspx?k=
"Information%20and%20communication"%20(CLISLegislationYear>

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
cybersecurity.ncb.mu (cyber security portal- knowledge bank on: online safety, sexting, sextortion + Guidelines on wide range of issues- e.g. social media attack, defamatory comments.
cert-mu.org
mcti.gov.mu.org – (National Cybersecurity Strategy 2014-2019)
https://www.lexpress.mu/.../cyberbullying-akash-callikan-porte-plai...
Draft National Cybercrime Strategy 2017-2020.

1. Country: Mauritius

2. Name of the Court: Intermediate Court

3. Date of the decision: 26 September 2012

4. Case number: CN 858/09

5. Parties to the case: Police v/s Bahadoor

6. Decision available on the Internet? ☒Yes ☐ No
https://supremecourt.govmu.org/_Layouts/CLIS.DMS/Search/NewSearchDoc2.aspx?
IsDlg=1&List=J&ID=286680&searchkey=Bahadoor

7. Topics /Key terms:
Indecent photographs, Sodomy, Sexual abuse

8. Summary of the facts (as reflected in the decision):

Accused was giving private tuition after school hours to students who had failed the sixth standard Certificate of Primary Education exams. He asked complainant, a minor, to come alone for tuitions

whereby he caused him to be sexually abused.
He caused the minor complainant to suck his private parts and kiss him on his lips. Accused used a camera, to take live pictures of the acts, by holding it with his right hands. Accused also took indecent photographs of the complainant who lied naked upon being directed by the accused about the posture he should adopt. He gave complainant money, gifts and chocolate for him not to relate the matter to anyone.

Following an enquiry by the Ombudsperson for children, the minor and his brother were brought for enquiry and they related everything in details, as a result of which police started its enquiry.

During the enquiry, Police found and secured indecent photographs of other children on the Accused's system unit and pen drive and those were taken with his camera.

9. Summary of applicable legal provision(s) and of reasoning of the Court:

14. Sexual offences

(1) Any person who causes, incites or allows any child to—

(a) be sexually abused by him or by another person;

shall commit an offence.

(2) For the purposes of subsection (1) (a), a child shall be deemed to be sexually abused where he has taken part whether as a willing or unwilling participant or observer in any act which is sexual in nature for the purposes of—

(a) another person's gratification;

(b) any activity of pornographic, obscene or indecent nature;

(c) any other kind of exploitation by any person.

15. Indecent photographs of children

(1) Any person who—

(a) takes or permits to be taken or to make, any indecent photograph or pseudo-photograph of a child;

The charges under counts in relation to taking indecent photographs of children were also proved since the photographs spoke for themselves. Counsel for the defence did not dispute that it was the accused who took all these photographs. The indecent character of such photographs was undeniable and was sufficient to establish the charge under both counts of the information.
Also the court noted that the accused focused the lens of his camera on shooting his subject, which he later fed in his pen drive.

Accused was found guilty on the charges referred and was sentenced to 12 months imprisonment.

https://supremecourt.govmu.org/Search/Pages/LegislationSearchResult.aspx?k="child%20protection%20act"%20(CLISLegislationYear>=2003%20AND%20CLIS

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
cybersecurity.ncb.mu (cyber security portal- knowledge bank on: online safety, sexting, sextortion + Guidelines on wide range of issues- e.g. social media attack, defamatory comments.
cert-mu.org
mcti.gov.mu.org – (National Cybersecurity Strategy 2014-2019)
https://www.lexpress.mu/.../cyberbullying-akash-callikan-porte-plai...
Draft National Cybercrime Strategy 2017-2020.

1. Country: Mauritius	
2. Name of the Court: Intermediate Court	
3. Date of the decision: 28 March 2012	**4. Case number:**
5. Parties to the case: Police v/s Teeluck	
6. Decision available on the Internet? ☒Yes ☐ No https://www.lexpress.mu/article/amendes-de-rs-150-000-%C3%A0-un-graphiste-pour-avoir-pirat%C3%A9-la-page-facebook-d%E2%80%99une-mineure	
7. Topics /Key terms: Identity theft, fake profile, threatening emails, interception of mail box, indecent photographs, fake message soliciting men for immoral purposes.	
8. Summary of the facts (as reflected in the decision): A graphic designer illegally intercepted the web page of a minor student of 15 years, modified her email address, intercepted her email box and posted indecent photographs of the minor on Facebook. As a result of those posts the complainant started to receive threatening emails as well as threat of sexual assaults. They even found on her Facebook account posts of her soliciting men for sexual purposes. She complained to the police who started an enquiry. Judicial order was sought and obtained for the purpose of the enquiry. The computer of the accused was verified both at his residence and workplace. Forensic examination of the computer system revealed incriminating evidence against the accused and confirmed the version of the complainant.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: **Information and Communication Technologies Act 2001** *Section 46(h) (ii) of the ICTA reads:* *"Any person who…* *(h) uses an information and communication service, including telecommunication service, -* *(ii) for the purpose of causing annoyance, inconvenience or needless anxiety to any person;* *shall commit an offence."* **Computer Misuse and Cybercrime Act 2003** **5. Unauthorised access to and interception of computer service** (1) Subject to subsection (5), any person who, by any means, knowingly— (a) secures access to any computer system for the purpose of obtaining, directly or indirectly, any computer service; (b) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within, a computer system, **6. Unauthorised modification of computer material** (1) Subject to subsections (3) and (4), any person who knowingly does an act, which causes an unauthorised modification of data held in any computer system shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to penal servitude for a term not exceeding 10 years. (2) Where as a result of the commission of an offence under this section— (a) the operation of the computer system; (b) access to any program or data held in any computer; or	

(c) the operation of any program or the reliability of any data,

Child Protection Act 1994

14. Sexual offences

(1) Any person who causes, incites or allows any child to—

(a) be sexually abused by him or by another person;

shall commit an offence.

(2) For the purposes of subsection (1) (a), a child shall be deemed to be sexually abused where he has taken part whether as a willing or unwilling participant or observer in any act which is sexual in nature for the purposes of—

(a) another person's gratification;

(b) any activity of pornographic, obscene or indecent nature;

(c) any other kind of exploitation by any person.

15. Indecent photographs of children

(1) Any person who—

(a) takes or permits to be taken or to make, any indecent photograph or pseudo-photograph of a child;

Accused was prosecuted and subsequently pleaded guilty.
In view of his guilty plea and the damning forensic evidence accused was sentence on the 28 March 2012 to pay a fine of Rs 150,000 in lieu of imprisonment.

https://supremecourt.govmu.org/Search/Pages/LegislationSearchResult.aspx?k=
"computer%20misuse"%20(CLISLegislationYear>=2003%20AND%20CLISLegislat

https://supremecourt.govmu.org/Search/Pages/LegislationSearchResult.aspx?k=
"Information%20and%20communication"%20(CLISLegislationYear>

https://supremecourt.govmu.org/Search/Pages/LegislationSearchResult.aspx?k=
"child%20protection%20act"%20(CLISLegislationYear>=2003%20AND%20CLIS

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☒
Article 3 – Illegal interception ☒
Article 4 – Data interference ☒
Article 5 – System interference ☒
Article 6 – Misuse of devices ☒
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
cybersecurity.ncb.mu (cyber security portal-knowledge bank on: online safety, sexting, sextortion + Guidelines on wide range of issues- e.g. social media attack, defamatory comments.
cert-mu.org
mcti.gov.mu.org – (National Cybersecurity Strategy 2014-2019)
https://www.lexpress.mu/article/amendes-de-rs-150-000-%C3%A0-un-graphiste-pour-avoir-pirat%C3%A9-la-page-facebook-d%E2%80%99une-mineure
https://www.lexpress.mu/.../cyberbullying-akash-callikan-porte-plai...
Draft National Cybercrime Strategy 2017-2020.

5.6.9 The Netherlands

1. Country: The Netherlands	
2. Name of the Court: Rechtbank Amsterdam (district court of Amsterdam)	
3. Date of the decision: March, 16, 2017	**4. Case number:** 13/995008-13
5. Parties to the case: Case name = Disclosure	
6. Decision available on the Internet? ☒Yes ☐ No http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBAMS:2017:1627	
7. Topics /Key terms: e.g. cyberbullying, cyberviolence, grooming, sexting, sexual assault and extortion	
8. Summary of the facts (as reflected in the decision): Conviction of a 39 year old male, Aydin C., for charges of production / possession of images of child sexual abuse, sexual assault of 34 girls, and for charges of extortion of an adult, as well as charges of hacking, fraud and possession of drugs. Sentence is 10 years, 8 months of imprisonment. He "abused dozens of young girls by gaining their trust through speaking with them on the internet," the court said. "He then abused that trust by forcing them to perform sexual acts before their webcams. If they refused to do it again, he threatened to send their images to their relatives or to publish them on pornography sites." Some of the victims were harassed for years, the court heard.	
9. Summary of applicable legal provision(s) and of reasoning of the Court; Dutch criminal code articles 240 b, 246 and 248a (Child sexual abuse); 1381b and 139d (hacking); 326 (fraud and extortion)	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☒ Article 10 – Offences related to infringements of copyright and related rights ☐	
11. Useful online link(s):	

5.6.10 Philippines

1. Country: Philippines	
2. Name of the Court: Branch 100, Regional Trial Court of Quezon City	
3. Date of the decision: May 29, 2017	**4. Case number:** R-QZN-15-00619-23-CR; R-QZN-15-03829-CR
5. Parties to the case: People of the Philippines v. Jerrie R. Arraz	
6. Decision available on the Internet? ☒**Yes** ☐ **No** https://drive.google.com/file/d/0B0y3WmFVmgWccDdNUDB3OEpjanc/view?usp=drive_web	
7. Topics /Key terms: Online Sexual Exploitation, Cyber Trafficking, Pornography, Cybersex, Rape	
8. Summary of the facts (as reflected in the decision): In October 2014, the private complainant, 19 years old, arrived at the Women and Children Protection Unit of the Criminal Investigation and Detection Group (WCPU-CIDG) alleging that she had been sexually abused by the accused, Jerrie Arraz. According to her, Jerrie Arraz deceived her into thinking she was only going to work as a domestic helper in his house where she resided in March 2014. She disclosed that Jerrie Arraz, by threat and use of force, compelled her to have sex with him, his relatives, and his customers. She further described that she was pregnant and intoxicated during some of these sexual encounters. The rapes began in March 2014, only weeks after she arrived, and continued until she left his residence in late June or early July 2014. The private complainant described in detail how Arraz maintained, transported, offered, and provided her to his customers by force, threat, and fraud between March and June 2014. The encounters were both in person at local hotels, and in the Arraz residence—**transmitted live** to his customers **via the internet**. Arraz made her believe she will be paid a certain amount in all the transactions however, Arraz pocketed all, if not most, of the proceeds of these transactions. She further complained that Arraz compelled her to pose naked or to perform explicit sexual acts in front of Arraz's digital camera, and computer webcam. Arraz would then send these lewd photos to his customers for profit and for his customers' pleasure. She further alleged that others, including her younger sister, were subjected to the same form of criminal abuse.	
9. Summary of applicable legal provision(s) and of reasoning of the Court **Violation of Section 4(a)(e), R.A. 10364.** "In the recent case of *People v. Hirang*, the Supreme Court defined the elements of trafficking in persons, as derived from the aforequoted Section 3(a), to wit: (1) The act of "recruitment, transportation, transfer or harboring or receipt of persons with or without the victim's consent or knowledge, within or across national borders"; (2) The means used which include "threat or use of force, or other forms of coercion, abduction, fraud, deception, abuse of power or of position, taking advantage of the vulnerability of the person, or, the giving or receiving of payments or benefits to achieve the consent of a person having control over another"; and (3) The purpose of trafficking is exploitation which includes "exploitation or the prostitution of others or other forms of sexual exploitation, forced labor or services, slavery, servitude or the removal or sale of organs." All these elements concur in these two cases. *First*. As to the act. As established by the evidence of the People, private complainant, clueless as she was, sought refuge in the perceived safety of the home of accused in March 2014. Her trust and confidence upon accused was further heightened with a promise of better future as accused would	

be giving her salary for taking care of his children and doing household chores. Little did private complainant know that her asking for help from accused would be the start of her Calvary. Under the circumstances, while accused did not recruit private complainant, he, however, clearly, maintained and hired the latter.

Second. As to the means. As records would reveal, private complainant participated in the acts complained of because of the fear that she would be thrown out of accused's house if she did not cooperate. If that happens, she has no one and place to turn to. It must be emphasized again that private complainant went to accused to have protection. Thus, when the same purpose is removed from the equation, she is helpless and vulnerable. It is this state of defencelessness that accused took advantage of. This is the means employed by accused. Aside from this, accused forced her to perform the purposes to be discussed below.

Third. As to the purpose. It is without doubt that the purpose of accused is for sexual exploitation. Private complainant narrated with specifics how accused manipulated, if not forced and coerced her to undress and pose, and have sexual contacts with him while the web camera had been on. He both took photos of the same lascivious poses and activities for him to post later in the internet for the consumption and enjoyment of his clients whom he shared the same perverse passion, if not twisted interest; and gave a live feed to this foreigner clients watching at the other end of the line fondling their own private part."

Cybersex (Section 4c, par. 1, R.A. 10175)

"Based on the narration of private complainant as well as the other witnesses for the People, which if taken together, lead this Court to reasonably conclude that the same was likewise violated by accused. To reiterate, he paraded the nude body of private complainant, ergo her private organs; and the latter's and his sexual activities, either live or still photos in the internet with the use of computer system, all for money. Clearly, accused was engaged in the business of trading flesh through the internet."

Rape (Art. 266-A, RPC)

"Be that as it may, the statement of private complainant as mentioned above and to be stated below, which were given in a categorical, straightforward, spontaneous and frank manner, deserves great weight and thus accorded credence."

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):

News report on the conviction from Inquirer: http://newsinfo.inquirer.net/900017/life-in-prison-for-demon-who-kept-kids-as-sex-slaves

5.6.11 Slovakia

1. Country: Slovakia	
2. Name of the Court: District Court Poprad	
3. Date of the decision: **15 May 2017**	**4. Case number:** 5T/25/2017
5. Parties to the case: n/a	
6. Decision available on the Internet? ☒Yes ☐ No https://obcan.justice.sk/infosud/-/infosud/i-detail/rozhodnutie/f71d5ff7-d350-415e-b2a1-4342ebd3486a%3A2188c88a-99ea-4a52-b950-cacf506feb37?_isufront_WAR_isufront_parentDetailPart=rozhodnutia&_isufront_WAR_isufront_parentEntityPk=160	
7. Topics /Key terms: Sexting, social networks, child pornography	
8. Summary of the facts (as reflected in the decision): A Person was found guilty for production of child pornography, sexual exploitation and distribution of child pornography. - Between 2013 until January 2016, he downloaded more than 3.000 files of child pornography through TOR network which he distributed via internet to other unknown users. - He persuaded several minor children (girls) via internet to pose nude while watching them via webcam, he recorded these videos and consequently stored in his computer. - Persuaded a minor (girl) to meet him for the purposes of taking naked pictures of her. He made several photos and stored them in his computer. - For financial compensation persuaded a mother of 3 children (children under age 12) to make photos of her children. In those images, there were details of their genital organs. Consequently, mother sent the photos several times via Skype. The mother also persuaded her daughter to pose nude in front of webcam, touching her genitals and the mother was doing the same. The perpetrator recorded these videos and stored them in his computer. - Persuaded other woman to come to his house to take pictures of her young daughter (2,5 years old) for financial compensation. The mother allowed this. The daughter was completely naked, pictures with detailed genitals. The woman was assisting and positioning her daughter. Furthermore, the woman came to his house with her daughter where he sexually exploited the daughter although the daughter was crying and trying to stop him, he took video of this. The mother was providing him with assistance. He took photos of a minor girl and under threats that he would show these photos to her family, teachers and schoolmates, was performing sex practices with her, making videos and photos. This has lead consequently to suicidal thoughts and psycho-sexual disorders of the girl.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: Section 201 of Criminal Code – sexual exploitation Section 368 – production of child pornography Section 369– distribution of child pornography Section 200 – sexual violence **Sentence imposed: 14 years**	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐	

Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):

Newspaper articles online: https://www.cas.sk/clanok/549628/martin-sa-priznal-k-otrasnemu-cinu-za-11-zneuzitych-deti-dostal-takyto-trest/

http://www.pluska.sk/regiony/vychodne-slovensko/kauza-zvrhlikov-z-detskeho-porna-neuhadnete-kto-upozornil.html

http://www.pluska.sk/krimi/krimi/kauza-zvrhlikov-z-detskeho-porna-jedna-z-matiek-roka-urobila-necakany-krok.html?utm_source=Pluska-2014&utm_medium=citajteviac&utm_campaign=vb2014

1. Country: Slovakia

2. Name of the Court: District Court Lučenec

3. Date of the decision: 25 January 2017

4. Case number: 3T/1/2017

5. Parties to the case: n/a

6. Decision available on the Internet? ☒Yes ☐ No
https://obcan.justice.sk/infosud/-/infosud/i-detail/rozhodnutie/c3388921-b8bf-4d42-8834-b46c2c69db2f%3A7d9cd59a-0e3d-4718-a8d4-57e0b06a16c9

7. Topics /Key terms:
Cyberviolence, social networks

8. Summary of the facts (as reflected in the decision):

A person was found guilty that from September 2015 to January 2017 he used website www.pokec.sk (Slovak social network used for chat) where he sent under his nickname messages to a woman stating that she is "a whore", "a prostitute" "and that she likes sex" and "she offers sexual services." This information was publicly accessible. He sent text messages to several males and shared telephone number, address of residence, address of employment of the female. He was sharing also inaccurate data which could endanger dignity of the victim. Furthermore, the perpetrator sent messages through Facebook chat and SMS messages to the victim stating that she is a "whore" and threatening her that he will go to her superior and inform him that she "offers sexual services." Furthermore, he said to her that he would not stop giving her telephone number through social networks with a note that she offers sexual services.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
Section 373 para 1,2 letter c of Criminal Code – defamation
Section 360a para 1 letter a,c of Criminal Code – dangerous stalking

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐

Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s): N/A.]

1. Country: Slovakia	
2. Name of the Court: District Court Prievidza	
3. Date of the decision: 24 March 2017	**4. Case number: 0T/30/2017**
5. Parties to the case: n/a	
6. Decision available on the Internet? ☒Yes ☐ No https://obcan.justice.sk/infosud/-/infosud/i-detail/rozhodnutie/afb47159-9415-4085-a8b3-00b50e4c3eb9%3A4a13d884-3584-4ca6-8e35-4466b2365e7c	
7. Topics /Key terms: Sexting, social networks	
8. Summary of the facts (as reflected in the decision): From October 2016 until March 2017, the accused was stalking his former girlfriend. He was repeatedly contacting her by his mobile phone by sending text messages and also through Facebook Messenger despite the fact that she asked him to stop. He was addressing demands to her to renew their relationship followed by threats that he will make public a private video of her with intimacy content. He was also threatening that he will show this video to her current partner.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: dangerous stalking, Section 360a para 1 letter b, c and para 2 letter a) of Act 300/2005 Criminal Code of Slovak Republic	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐	
11. Useful online link(s):	

1. Country: Slovakia	
2. Name of the Court: District Court Stara Lubovna	
3. Date of the decision: 12 September 2016	**4. Case number: 1T/87/2016**

5. Parties to the case: n/a	
6. Decision available on the Internet? ☒Yes ☐ No https://obcan.justice.sk/infosud/-/infosud/i-detail/rozhodnutie/41e4b2be-4d6f-423e-ae12-775f7d9ed447%3A44f246df-f3fa-49ee-afad-8c2fd3569d44	
7. Topics /Key terms: Sexting, social networks, child pornography	
8. Summary of the facts (as reflected in the decision): A person was found guilty that from September 2013 until February 2016 he was repeatedly by various means sexually exploiting (at least once a week) his minor sister despite the fact that he knew she was not 12 years old. He was making photos and videos while performing these acts and then he saved the photos and videos on his computer. In 2015 and 2016, through a website azet.sk (used for chat) he sent these photos under his nickname to several persons through instant messaging and emails.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: Section 201 para 1, 2 letter a) and b) of Criminal Code – sexual exploitation Section 368 para 1,2 letter a) and b) – production of child pornography Section 369 para 1, 2 letter a) and b) – distribution of child pornography Sentence imposed: 7 years	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☒ Article 10 – Offences related to infringements of copyright and related rights ☐	
11. Useful online link(s):	

1. Country: Slovakia	
2. Name of the Court: District Court Presov	
3. Date of the decision: 17 June 2016	**4. Case number: 41T/30/2016**
5. Parties to the case: n/a	
6. Decision available on the Internet? ☒Yes ☐ No https://obcan.justice.sk/infosud/-/infosud/i-detail/rozhodnutie/fae6f3cb-7b18-4173-b42f-e49b7961571f%3A08e24495-9afe-4877-87f5-ba412ca7f66a	
7. Topics /Key terms: Sexting, social networks	

8. Summary of the facts (as reflected in the decision):

The accused made a photo album of a minor girl called "I bare," in which he placed at least 28 photos of a minor with pornographic character and made this photo album accessible to a group of 60 persons close to the victim who had been labeled as "friends," on the basis of which the parents of the victim got knowledge about all, at least as of 25 August 2013 MW, MSCM Czech Republic and elsewhere, which on the internet server www.azet.sk http://www.azet.sk appearing under the user name XXMINIX, after having gained access to the user account named B., created on the server http://www.azet.sk belonging to the minor victim B..V .., N .. XX.XX.XXXX, on which she had published her physical age at that time 14 years. Subsequently, he gained through access to the B..B e-mail address also minor´s account on the social network Facebook, where he then communicated with the victim through the chat server www.pokec.sk and also via the Skype, where he used the username ".V. and the V..V account name. He suggested her that he returns her access Pokec and to Facebook profiles, if she takes and sends him her 10 photos in the underwear what victim has agreed with and took them with her mobile phone at the place of her residence, and then sent about 10 photos through the Skype according to his requirements. However, the accused threatened to publish these photos as part of minor´s Facebook profile and making them unpublished under the condition of creating other photos on which she should be exposed naked in order to make visible her breasts and female genital organs. The minor girl has frightened of it and gradually was sending by her cell phone at the place of her residence photographs of her naked body according to his requirements. She sent him through Skype at least 73 photographs, however, the accused was still demanding additional photos, but in the period after 30 August 2013 she stopped communicating with him. He fulfilled his threats and published a part of these compromising photos in her Facebook profile at least from 13 July 2013.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
Section 368 para. 1, para. 2 letter b), - production of child pornography
Section 189 para. 1, para. 2 letter a), b), c), - extortion
Section 201 para. 1 – sexual exploitation

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):

1. Country: Slovakia

2. Name of the Court: District Court Vranov nad Toplou

3. Date of the decision: 15 February 2017

4. Case number: 12T/193/2016

5. Parties to the case: n/a

6. Decision available on the Internet? ☒Yes ☐ No

https://obcan.justice.sk/infosud/-/infosud/i-detail/rozhodnutie/7823fe7b-8cf5-484c-91f7-2832e33c17c7%3A8e63f5dc-6a25-44bb-97ec-98f22a95cd8f
7. Topics /Key terms: Social networks
8. Summary of the facts (as reflected in the decision): On 3 December 2015 for the purposes to discredit his former wife before public and her relatives, the accused created a profile on an internet portal, with photographs and contact details of his former wife, so it looked like the profile was created by her. He added also a note stating that she is offering sexual services, messages accepted. This should have created impression that the woman offers sexual services for remuneration although she had never engaged in such activities. The accused communicated false information about another person, which is capable of considerably damaging the respect of fellow citizens for such a person, her career and business, her family relations, or that causes her grievous harm
9. Summary of applicable legal provision(s) and of reasoning of the Court: Section 373, para 1, para 2, letter c) - Defamation
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s):

5.6.12 Slovenia

1. Country: Slovenia	
2. Name of the Court: Republika Slovenia, High court in Ljubljana	
3. Date of the decision: **7. 12. 2012**	**4. Case number:** VSL II Kp 9220/2011
5. Parties to the case: Appeal of the state prosecutor to the District Court's decision to remove evidence	
6. Decision available on the Internet? x Yes ☐ No http://www.sodisce.si/znanje/sodna_praksa/visja_sodisca/2012032113052385/#	
7. Topics /Key terms: e.g. cyberbullying; online violence, grooming, sexting, social networks sexual abuse of children on the Internet, dissemination of material showing sexual abuse of children	
8. Summary of the facts (as reflected in the decision): The essence of the case: The right to privacy cannot be absolute, but is limited by (constitutional) protection of the rights and benefits of others, in the concrete case of children. Sexual exploitation of children and child pornography constitute a serious violation of the human rights and fundamental rights of the child towards coherent education and development. Therefore, the established interference with the	

defendant's right to (communication) privacy, which was indeed due to the conduct of an operator who did not destroy the traffic data at the end of the statutory retention period, and which, according to a court order, could have been communicated to the police, in the particular case of minor importance in compared to the objective that justified the acquisition of traffic data from the operator, namely the disclosure of the perpetrator of a criminal offense prosecuted ex officio, with the prosecution being aimed at combating sexual abuse and sexual exploitation of children and the protection of children's rights to protection.

Summary from a court decision:
The Dutch police informed the Slovenian police of an operation related to the distribution of child pornographic material to access from a few thousand IP addresses to the server on which the perpetrators uploaded image files containing images of sexual abuse of children. It was found that they were seen by a Slovenian user among them. The user of the Slovenian IP address has viewed and transferred the disputed child files to him. The tracing of the perpetrator required information on the participants, circumstances and facts of the electronic communications traffic.

On the pre-trial hearing, on the basis of the third paragraph of Article 385.e of the CPA, the Court of First Instance decided to exclude from the file all the evidence obtained against the suspect B.M. in the pre-trial procedure because he considered that it had been obtained through a violation of the defendant's right to privacy, set out in Article 35 of the Constitution of the Republic of Slovenia.

The Court of Appeal ruled that the concealed investigative measure of obtaining data in the electronic communications network (Article 149b, first paragraph of ZKP) was ordered and executed legally.

Under the Constitution, the human rights and fundamental freedoms of children enjoying special protection and care before economic, social, physical, mental or other exploitation and abuse are particularly protected (Articles 35 and 56 of the Constitution of the Republic of Slovenia). In the criminal offense under Article 176 of the KZ-1, there is a gross interference with the safety, physical and sexual integrity of minors, who are often victims of perpetrators, including organized crime, exploiting the most vulnerable part of the human population.

9. Summary of applicable legal provision(s) and of reasoning of the Court: [Add references or links applicable legislation(s) and specific article(s) possibly in English]
http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050 (English version - button on the right/top)
http://www.us-rs.si/en/about-the-court/legal-basis/ (II. Paragraph)
http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography x
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
http://www.sodisce.si/znanje/sodna_praksa/visja_sodisca/2012032113052385/#

Subsequently, the Constitutional Court of the Republic of Slovenia decided on 3 July 2013 that data retention was unconstitutional and, on this basis, decided that the retention provisions of the Electronic Communications Act would be settled, while at the same time it would be imposed on operators, Internet service providers to destroy all data that they have kept on the basis of repealed tax provisions. This decision (http://odlocitve.us-rs.si/sl/location/US30439) came into force on 11 July 2014. Since then, Slovenia has no retention data.

5.6.13 United States of America

1. Country: United States of America	
2. Name of the Court: U.S. District Court for the Eastern District of Michigan	
3. Date of the decision: 23/04/2014	**4. Case number:** 13CR20522-1
5. Parties to the case: United States v. Adam Paul Savader	
6. Decision available on the Internet? ☒**Yes** ☐ **No** http://documents.tips/documents/adam-savader-sentencing-judgment.html	
7. Topics /Key terms: Cyberstalking; Internet extortion	
8. Summary of the facts (as reflected in the decision): In 2012 and 2013, Adam Savader hacked into the email accounts of victims in at least three different states. After accessing the email accounts, all of which belonged to women that Savader knew, he stole nude or partially nude images from those accounts and extorted and harassed young women using the stolen photos. Savader threatened to release the nude photos of the young women if the young women did not send him additional pornographic photos. He was sentenced to 30 months of imprisonment and 36 months of probation period.	
9. Relevant domestic legislation(s) and specific article(s): **18 U.S.C. § 2261(a)(2) and 18 U.S.C. § 2261(b)** (a) Whoever – (1) travels in interstate or foreign commerce or is present within the special maritime and territorial jurisdiction of the United States, or enters or leaves Indian country, with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, and in the course of, or as a result of, such travel or presence engages in conduct that— (A) places that person in reasonable fear of the death of, or serious bodily injury to— (i) that person; (ii) an immediate family member (as defined in section 115) of that person; or (iii) a spouse or intimate partner of that person; or (B) causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person described in clause (i), (ii), or (iii) of subparagraph (A); or * * * * shall be punished as provided in section 2261(b) of this title. * * * * **18 U.S.C. § 875(d)** (d) Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both.	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☒ Article 3 – Illegal interception ☒ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☒ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐	
11. Useful online link(s): https://archives.fbi.gov/archives/detroit/press-releases/2013/new-york-man-charged-with-internet-extortion-and-cyber-stalking http://www.villagevoice.com/news/former-romney-intern-adam-savader-pleads-guilty-to-cyberstalking-one-woman-wont-face-trial-for-the-other-14-6682671	

http://www.politico.com/story/2013/04/ex-romney-intern-arrested-blackmail-090552
http://theislandnow.com/news-98/savader-gets-30-month-jail-sentence/

1. Country: United States of America

2. Name of the Court: U.S. District Court for the Central District of California

3. Date of the decision: 28/08/2009

4. Case number: 08-CR-582

5. Parties to the case: United States v. Drew

6. Decision available on the Internet? ☒**Yes** ☐ **No**
http://www.dmlp.org/sites/citmedialaw.org/files/2009-08-28-Opinion%20on%20Drew%27s%20Rule%2029%28c%29%20Motion_0.pdf

7. Topics /Key terms:
Cyberbullying; MySpace, suicide

8. Summary of the facts (as reflected in the decision): [no more than 200 words]

On May 15, 2008, Lori Drew was indicted in federal court in California for her alleged role in a hoax on MySpace directed at Megan Meier, a 13-year-old neighbor of Drew's who committed suicide in October 2006 after a "boy" she met on MySpace abruptly turned on her and ended their relationship. The boy was allegedly Lori Drew, who pretended to be 16-year-old "Josh Evans" to gain the trust of Megan, who had been fighting with Drew's daughter.
The grand jury charged Drew with conspiracy and three counts of accessing protected computers without authorization in violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 for violation of MySpace's Terms of Services. In particular, the jury did find Defendant "guilty" "of [on the dates specified in the Indictment] accessing a computer involved in interstate or foreign communication without authorization or in excess of authorization to obtain information in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(A), a misdemeanor."
The Judge of the case, however, ruled that accepting the government's theory — and the jury's finding — that Drew violated the CFAA merely by intentionally violating MySpace's terms of use would render the statute unconstitutionally vague. As a result, he granted Drew's motion for a judgment of acquittal, ending the government's case against her, and issued an opinion on 28th of August 2009 overturning the jury verdict on the consideration that "if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law «that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet].» City of Chicago, 527 U.S. at 64."

9. Relevant domestic legislation(s) and specific article(s):
Computer Fraud and Abuse Act - 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii),

(a) Whoever –
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains –
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.)
(B) information from any department or agency of the United States; or
(C) information from any protected computer if the conduct involved an interstate or foreign communication;
* * * *
shall be punished as provided in subsection (c) of this section.
* * * *
(c) The punishment for an offense under subsection (a) or (b) of this section is –
* * * *
(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if –
(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
(iii) the value of the information obtained exceeds $5,000

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☒
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
https://www.meganmeierfoundation.org/megans-story.html
https://en.wikipedia.org/wiki/Suicide_of_Megan_Meier
http://www.dmlp.org/threats/united-states-v-drew
https://nobullying.com/the-megan-meier-story/

1. Country: United States of America

2. Name of the Court: U.S. District Court for the Central District of California

3. Date of the decision: 16/09/2011

4. Case number: 10-743-GHK

5. Parties to the case: United States v. Mijangos

6. Decision available on the Internet? ☒**Yes** ☐ **No**
https://www.docketalarm.com/cases/California_Central_District_Court/2--10-cr-00743/USA_v._Mijangos/76/

7. Topics /Key terms:
Sextortion; Malware; Pornography

8. Summary of the facts:

Luis Mijangos was a 32-year-old computer hacker who infected the computers of hundreds of victims by sending trojan emails and instant messages ("IMs") embedded with malicious software that gave him complete access to and control over the victims' computers.
Defendant repeatedly committed such acts for over a year and a half, using this access to steal victims' financial information and other personal information used for identity theft.
He used also this access to read victims' emails and IMs, watched them through their webcams, and listened to them through the microphones on their computers.
Often, he used the intimate images or videos of female victims he stole from the victims' computer to "sextort" those victims, threatening to post those images/videos on the Internet unless the victims provided more to defendant.
He also forced victims into creating pornographic images/videos by assuming the online identity of victims' boyfriends. Dozens of the victims were minors at the time of the facts.
He was found guilty and had been convicted as charged of the offences of accessing protected computers to obtain information, aiding and abetting and causing an act to be done and wiretapping.

9. Relevant domestic legislation(s) and specific article(s):
18 U.S.C. §§ 1030(a)(2)(C)

(a) Whoever –
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains –
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.)

(B) information from any department or agency of the United States; or
(C) information from any protected computer if the conduct involved an interstate or foreign communication;

18 U.S.C. 2511(1)(a)

(1) Except as otherwise specifically provided in this chapter any person who—
(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
* * * *
shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☒
Article 3 – Illegal interception ☒
Article 4 – Data interference ☒
Article 5 – System interference ☒
Article 6 – Misuse of devices ☒
Article 7 – Computer-related forgery ☒
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☒
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
https://www.justice.gov/archive/usao/cac/Pressroom/pr2010/097.html
http://latimesblogs.latimes.com/lanow/2011/09/sextortion-six-years-for-oc-hacker-who-forced-women-to-give-up-naked-pics-.html
https://archives.fbi.gov/archives/losangeles/press-releases/2011/orange-county-man-who-admitted-hacking-into-personal-computers-sentenced-to-six-years-in-federal-prison-for-sextortion-of-women-and-teenage-girls
http://www.nydailynews.com/news/national/luis-mijangos-6-years-hacking-women-computers-blackmailing-explicit-photos-article-1.956630
http://www.ocweekly.com/news/updated-luis-mijangos-guilty-of-being-sextortion-hacker-6472087

1. Country: United States of America

2. Name of the Court: United States District Court for the Northern District of Georgia

3. Date of the decision: Dec 9, 2015

4. Case number: 1:15CR319

5. Parties to the case: United States v. Michael Ford

6. Decision available on the Internet? ☐Yes ☒ No
No written decision.

7. Topics /Key terms:
sextortion, cyberstalking, social media

8. Summary of the facts (as reflected in the decision): In 2016, federal prosecutors obtained a 57-month sentence for Michael C. Ford who, while employed by the Department of State at the London embassy, engaged in a widespread, international computer hacking, cyberstalking, and "sextortion" campaign. Ford sent "phishing" emails to thousands of potential victims, warning them that their e-mail accounts would be deleted if they did not provide their passwords. Ford then hacked into hundreds of e-mail and social media accounts using the passwords collected from his phishing scheme, where he searched for sexually explicit photographs. Once Ford located such photos, he then searched for personal identifying information (PII) about his victims, including their home and work addresses, school and employment information, and names and contact information of family members, among other things. Ford then used the stolen photos and PII to engage in an ongoing cyberstalking campaign designed to demand additional sexually explicit material and personal information. Ford e-mailed his victims with their stolen photos attached and threatened to release those photos if they did not cede to his demands. When the victims refused to comply, threatened to go to the police or begged Ford to leave them alone, Ford responded with additional threats. For example, Ford wrote in one e-mail "don't worry, it's not like I know where

you live," then sent another e-mail to the same victim with her home address and threatened to post her photographs to an "escort/hooker website" along with her phone number and home address. Ford later described the victim's home to her, stating "I like your red fire escape ladder, easy to climb." Ford followed through with his threats on several occasions, sending his victims' sexually explicit photographs to family members and friends. Ford pled guilty to violations of 18 U.S.C. 2261(A)(2)(B) (cyberstalking), 1030(a)(7) (extortion), and 1343 (wire fraud).

9. Summary of applicable legal provision(s) and of reasoning of the Court:
18 U.S.C. 2261(A)(2)(B) (cyberstalking) https://www.law.cornell.edu/uscode/text/18/2261A
18 U.S.C. 1030(a)(7) (extortion) https://www.law.cornell.edu/uscode/text/18/1030
18 U.S.C. 1343 (wire fraud) https://www.law.cornell.edu/uscode/text/18/1343

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☒
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
https://www.justice.gov/opa/pr/former-us-state-department-employee-sentenced-57-months-extensive-computer-hacking

1. Country: United States of America

2. Name of the Court: United States District Court for the District of Delaware

3. Date of the decision: July 10, 2015

4. Case number: 1:13 CR 83

5. Parties to the case: United States v. Matusiewicz

6. Decision available on the Internet? ☒Yes ☐ No
http://www.leagle.com/decision/In%20FDCO%2020151222B22/U.S.%20v.%20MATUSIEWICZ

7. Topics /Key terms:
cyberstalking

8. Summary of the facts (as reflected in the decision):
In 2016, federal prosecutors obtained three life sentences for defendants David Matusiewicz, Lenore Matusiewicz, and Amy Gonzalez, in the first case to allege 18 U.S.C. § 2261A's "resulting in death" enhancement. The defendants were charged with multiple acts violating 18 U.S.C. §§ 2261A(1) and 2261(2) (interstate stalking and cyberstalking), 18 U.S.C. § 371 (conspiracy). The defendants engaged in a prolonged campaign to surveil and harass Thomas Matusiewicz's ex-wife as the result of the termination of his parental rights. The online harassment included posting sexual abuse accusations against the victims online and sending these accusations to the victims' school and church. The defendants travelled to Delaware for a family court hearing where David Matusiewicz shot the victim, her companion, and himself.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
18 U.S.C. 2261A(1) https://www.law.cornell.edu/uscode/text/18/2261A
18 U.S.C. 2261(2) https://www.law.cornell.edu/uscode/text/18/2261
18 U.S.C. 371 https://www.law.cornell.edu/uscode/text/18/371

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐

Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐
11. Useful online link(s): https://www.justice.gov/opa/pr/three-family-members-receive-life-sentences-courthouse-murder-conspiracy

1. Country: United States of America	
2. Name of the Court: United States District Court for the Central District of California	
3. Date of the decision: June 4, 2014	**4. Case number:** 753 D.3d 939 (2014)
5. Parties to the case: United States v. Christopher Osinger	
6. Decision available on the Internet? ☒Yes ☐ No http://cdn.ca9.uscourts.gov/datastore/opinions/2014/06/04/11-50338.pdf	
7. Topics /Key terms: Cyberstalking, sextortion, social media, revenge porn	
8. Summary of the facts (as reflected in the decision): In 2014, the Ninth Circuit affirmed the conviction and 46-month sentence of Christopher Osinger for violations 18 U.S.C. §§ 2261A(2)(A) and 2261(b)(5). Osinger sent the victim several threatening text messages, and he sent sexually explicit pictures of the victim to her fellow employees. He also created a Facebook page in a name close to the victim's and used the page to post suggestive and sexually explicit photos of the victim.	
9. Summary of applicable legal provision(s) and of reasoning of the Court: 18 USC 2261A(2)(A) https://www.law.cornell.edu/uscode/text/18/2261A 18 USC 2261(b)(5) https://www.law.cornell.edu/uscode/text/18/2261	
10. Possibly relevant provisions of the Budapest Convention: Article 2 – Illegal access ☐ Article 3 – Illegal interception ☐ Article 4 – Data interference ☐ Article 5 – System interference ☐ Article 6 – Misuse of devices ☐ Article 7 – Computer-related forgery ☐ Article 8 – Computer related fraud ☐ Article 9 – Offences related to child pornography ☐ Article 10 – Offences related to infringements of copyright and related rights ☐	
11. Useful online link(s):	

1. Country: United States of America	
2. Name of the Court: United States District Court for the District of Maine, United States Court of Appeals for the First Circuit	
3. Date of the decision: May 2, 2014	**4. Case number:** 748 F.3d 425
5. Parties to the case: United States v. Shawn Sayer	
6. Decision available on the Internet? ☒Yes ☐ No http://caselaw.findlaw.com/us-1st-circuit/1665132.html	
7. Topics /Key terms: cyberstalking	
8. Summary of the facts (as reflected in the decision): In 2012, federal prosecutors obtained an indictment alleging that Shawn Sayer violated 18 U.S.C. § 1028(a)(7) (identity theft) and § 2261A(2)(A) (cyberstalking). After pleading guilty pursuant to a	

plea agreement, Sayer received a statutory maximum five-year sentence under 18 U.S.C. § 2261A(2)(A). Sayer stalked his victim after their relationship ended. The victim obtained protective orders against the defendant, who had been arrested on at least eight prior occasions for violating the orders. The stalking escalated when Sayer posted pictures of the victim on Craigslist in the "Casual Encounters" section. In addition to the photos, the ads included directions to the home of the victim, causing her to be terrified for her safety.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
18 USC 1028(a)(7) https://www.law.cornell.edu/uscode/text/18/1028
18 USC 2261A(2)(A) https://www.law.cornell.edu/uscode/text/18/2261A

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):

1. Country: United States of America

2. Name of the Court: United States District Court for the District of Connecticut

3. Date of the decision: June 23, 2015

4. Case number: 3:15CR110

5. Parties to the case: United States v. Matthew Tollis

6. Decision available on the Internet? ☐Yes ☒ No
No published decision

7. Topics /Key terms:
Swatting

8. Summary of the facts (as reflected in the decision): In 2015, Matthew Tollis pled guilty to conspiring to engage in the malicious conveying of false information, namely a bomb threat hoax. Tollis and his co-conspirators placed hoax emergency calls reporting threats involving bombs, hostage taking, firearms, and mass murder at institutions such as the University of Connecticut, the Boston Convention and Exhibition Center, Boston University, two high schools in New Jersey, and a high school in Texas. The hoax call to University of Connecticut, for example, resulted in a three-hour, campus-wide lockdown and instigated a massive law enforcement response, including a Special Weapons and Tactics (SWAT) unit. Tollis was sentenced to one year and one day of imprisonment for his involvement in the conspiracy.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
18 USC 371 https://www.law.cornell.edu/uscode/text/18/371
18 USC 844(e) https://www.law.cornell.edu/uscode/text/18/844

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐

Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
https://www.fbi.gov/contact-us/field-offices/newhaven/news/press-releases/wethersfield-man-sentenced-to-prison-term-for-involvement-in-multiple-swatting-incidents

1. Country: United States of America

2. Name of the Court: United States District Court for the District of New Hampshire

3. Date of the decision: August 25, 2016

4. Case number: 1:15CR-115

5. Parties to the case: United States of America v. Ryan Vallee

6. Decision available on the Internet? ☐Yes ☒ No
There is no written decision, but the indictment is here: https://www.justice.gov/opa/file/631101/download.

7. Topics /Key terms:
Cyberbullying, sextortion, cyberstalking

8. Summary of the facts (as reflected in the decision): In 2016, federal prosecutors entered a plea agreement with Ryan J. Vallee, who pled guilty to violations of 18 USC 875(d) (interstate threats), 1030(a)(2)(C) (computer fraud), 1030(a)(7) (extortion), 1028A (aggravated identity theft), and 2261A(2)(B) (cyberstalking). Vallee remotely hacked into the online accounts of almost a dozen female victims and sent them threatening online communications, in some instances containing sexually explicit photos, in order to force the victims to send him sexually explicit photos of themselves. Vallee admitted that he repeatedly sent threatening electronic communications to his victims, usually by using spoofing or anonymizing text message services, in which he threatened his victims that unless they gave him sexually explicit photographs of themselves, he would continue with the above-described conduct. According to the admissions in the plea agreement, when most of the victims refused to comply with Vallee's demands and begged him to leave them alone, Vallee responded with threats to inflict additional harm. Vallee was sentenced to eight years of imprisonment.

9. Summary of applicable legal provision(s) and of reasoning of the Court:
18 USC 875(d) (interstate threats) https://www.law.cornell.edu/uscode/text/18/875
1030(a)(2)(C) (computer fraud) https://www.law.cornell.edu/uscode/text/18/1030
1030(a)(7) (extortion) https://www.law.cornell.edu/uscode/text/18/1030
1028A (aggravated identity theft) https://www.law.cornell.edu/uscode/text/18/1028A
2261A(2)(B) (cyberstalking) https://www.law.cornell.edu/uscode/text/18/2261A

10. Possibly relevant provisions of the Budapest Convention:

Article 2 – Illegal access ☒
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s):
https://www.justice.gov/opa/pr/new-hampshire-man-pleads-guilty-computer-hacking-and-sextortion-scheme-involving-multiple

1. Country:
United States

2. Name of the Court:
US Supreme Court

3. Date of the decision:
1 June 2015

4. Case number: 13-983, 575 U.S. __ (2015)

5. Parties to the case:
Anthony Elonis and the United States

6. Decision available on the Internet? x☐**Yes** ☐ **No**
https://www.supremecourt.gov/opinions/14pdf/13-983_7l48.pdf

7. Topics /Key terms:
e.g. cyberbullying; cyberviolence, grooming, sexting, social networks
threats posted publicly on Facebook

8. Summary of the facts (as reflected in the decision): Elonis posted on Facebook what he called rap lyrics with graphically violent language and imagery about his estranged wife, his co-workers, a kindergarten class, and state and federal law enforcement officers. For example, some posts talked about torturing his wife to death and carrying out a mass shooting of schoolchildren. Elonis often posted that these lyrics were fiction, were not intended to depict real people, and were protected by his rights under the US Constitution. Many who knew him saw the posts as threatening: his boss fired him, his wife obtained a court order keeping him away from her, and law enforcement began investigating him (during which he posted about murdering one of the FBI agents).
He was convicted of transmitting threats (see below) and the conviction was upheld on the first appeal. He then appealed to the highest US court, claiming that the posts had not been true threats, despite their effect on others, because he had not meant them.

9. Summary of applicable legal provisions and of reasoning of the court:
Section 875 (c) of Title 18 of the US Code.
Elonis was convicted of transmitting in interstate commerce [by posting on Facebook] a communication containing a "threat to injure the person of another." The Supreme Court voided his conviction because the government had not proven that he had had the necessary intent. The necessary intent would be that he had transmitted the communication either a) for the purpose of issuing a threat or b) with knowledge that the communication would be viewed as a threat.

10. Possibly relevant provisions of the Budapest Convention: none

Article 2 – Illegal access ☐
Article 3 – Illegal interception ☐
Article 4 – Data interference ☐
Article 5 – System interference ☐
Article 6 – Misuse of devices ☐
Article 7 – Computer-related forgery ☐
Article 8 – Computer related fraud ☐
Article 9 – Offences related to child pornography ☐
Article 10 – Offences related to infringements of copyright and related rights ☐

11. Useful online link(s): N/A