COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

9 July 2018
Strasbourg, France

T-CY(2017)10

Cybercrime Convention Committee (T-CY)

Working Group on cyberbullying and other forms of online violence, especially against women and children

Mapping study on cyberviolence

with recommendations adopted by the T-CY on 9 July 2018

www.coe.int/cybercrime

Contents

Contact

Alexander Seger
Executive Secretary of the Cybercrime Convention Committee (T-CY)
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France
Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email: alexander.seger@coe.int

1 Introduction

Acts of violence against individuals committed by means of or facilitated by information and communication technologies ("cyberviolence") have become a primary concern for societies and individuals.

T-CY 16 (Strasbourg, November 2016), therefore, decided:

- To note strong support for the establishment of a T-CY Working Group on cyberbullying and other forms of online violence, especially against women and children – based on article 1.1.j of the T-CY Rules of Procedure – and
- to task the Group to study the topic in the form of a mapping exercise, including comparative approaches to legislation as well as documentation of good practices in view of presenting interim results to the 17th Plenary and a final report to the 18th Plenary of the T-CY.[1]

The 18th Plenary in November 2017 then decided:

- To extend the mandate of the Working Group to 31 July 2018 and to request the Group to submit a final draft of the mapping study to T-CY 19 (July 2018) and to facilitate a workshop on this topic at the Octopus Conference in July 2018.

While cyberviolence may be targeted at any individual or group and may entail a wide range of acts, this mapping study focuses in particular on children and women, who are often the victims of cyberviolence. The experience and solutions with regard to these victims should modus modendi be applicable to other categories of victims while taking into account the specificities of violence against different categories of victims.[2]

The present study is thus aimed at:[3]

- mapping acts that constitute cyberviolence and drawing conclusions as to typologies and concepts;
- providing examples of national experiences and responses to such acts (including policies, strategies, legislation, cases and case law);
- discussing international responses under the Budapest Convention and other treaties (in particular the Istanbul and Lanzarote Conventions of the Council of Europe);
- developing recommendations as to the further course of action.

As a "mapping study" the present report is not intended to provide a complete and final analysis of the phenomenon of and responses to cyberviolence.

The study represents the findings of the Group and was taken note of by the 19th Plenary of the T-CY on 9 July 2018. The T-CY on that occasion adopted the "recommendations" and "follow up" as proposed in sections 4.2 and 4.3.

This study and possible follow up may also be considered to contribute to UN Agenda 2030 and the Sustainable Development Goals (SDGs), striving to "foster peaceful, just and inclusive societies which are free from fear and violence"[4].

[1] The Group included Markko KUNNAPU (Estonia), Erik PLANKEN (the Netherlands), Gareth SANSOM (Canada), Cristina SCHULMAN (Romania), Eirik Tronnes HANSEN (Norway), Branislav KADLECIK (Slovakia) and Laura-Kate BERNSTEIN (USA), and was supported by Betty SHAVE (Council of Europe consultant).
[2] For terminology related to the sexual exploitation and sexual abuse of children see the Luxembourg Guidelines (Terminology Guidelines for the Protection of Children From Sexual Exploitation and Sexual Abuse) adopted by an Interagency Working Group in Luxembourg on 28 January 2016).
http://luxembourgguidelines.org/english-version/
[3] One Party to the Budapest Convention does not agree with the scope of the study.

2 Mapping the phenomena

2.1 Overview of cyberviolence

2.1.1 Defining cyberviolence

Due to the potential breadth of the phenomena and the diversity of categories and sub-categories, determining the focus of this mapping exercise has been an ongoing challenge. The Working Group eventually reached consensus on using "cyberviolence" as the most concise term to be used consistently throughout the study, defining it as follows:

> Cyberviolence is the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities.[5]

Information received from Parties suggests that some countries have laws that specifically address particular forms of cyberviolence. Although cyberviolence has existed for some years, its specific forms seem to have only recently begun to be identified and understood. Most countries are struggling to recognize the different facets of the problem and to address them in domestic law.

It is critical to recall that many forms of cyberviolence are already covered in domestic or international law by "physical world" provisions, and investigations may not have to wait for new legislation.

For example, when computers are used to cause or facilitate violence through the transmission of messages that cause psychological harm, or through advertisement for murder, rape, kidnapping or trafficking in human beings, such cases may be prosecuted (depending on their facts) as assault, violation of privacy, illegal threat, extortion, solicitation of rape or murder, illegal distribution of content (such as photographs), domestic violence, and so on.

Furthermore, given the dependence on computer systems – including psychological, physical and economic dependence – some types of cybercrime (illegal access to intimate personal data, the destruction of data, etc.) may also be considered acts of cyberviolence.

---

[4] SDG 16 "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels"
https://sustainabledevelopment.un.org/post2015/transformingourworld
https://www.coe.int/en/web/un-agenda-2030/home

[5] This working definition is an adaptation of the "cyber" context of the definition of violence against women of Article 3 of the Istanbul Convention which defines it

> *as a violation of human rights and a form of discrimination against women and shall mean all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.*

Similarly, Article 1 of the Inter-American Convention on the prevention, punishment and eradication of violence against women (the Belém do Para Convention) defines violence against women as:

> *any act or conduct, based on gender, which causes death or physical, sexual or psychological harm or suffering to women, whether in the public or the private sphere.*

A comprehensive definition of violence against women is also provided by the United Nations:

> *Any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.*

http://www.un.org/womenwatch/daw/vaw/v-overview.htm
Common to all of these definitions is that "violence" is not limited to physical harm.
The members of the Working Group recognize that this working definition is rather broad and needs to mature further. On the other hand, it is a reality that any crime may have a "cyber" element that may change the nature and scope of the crime.

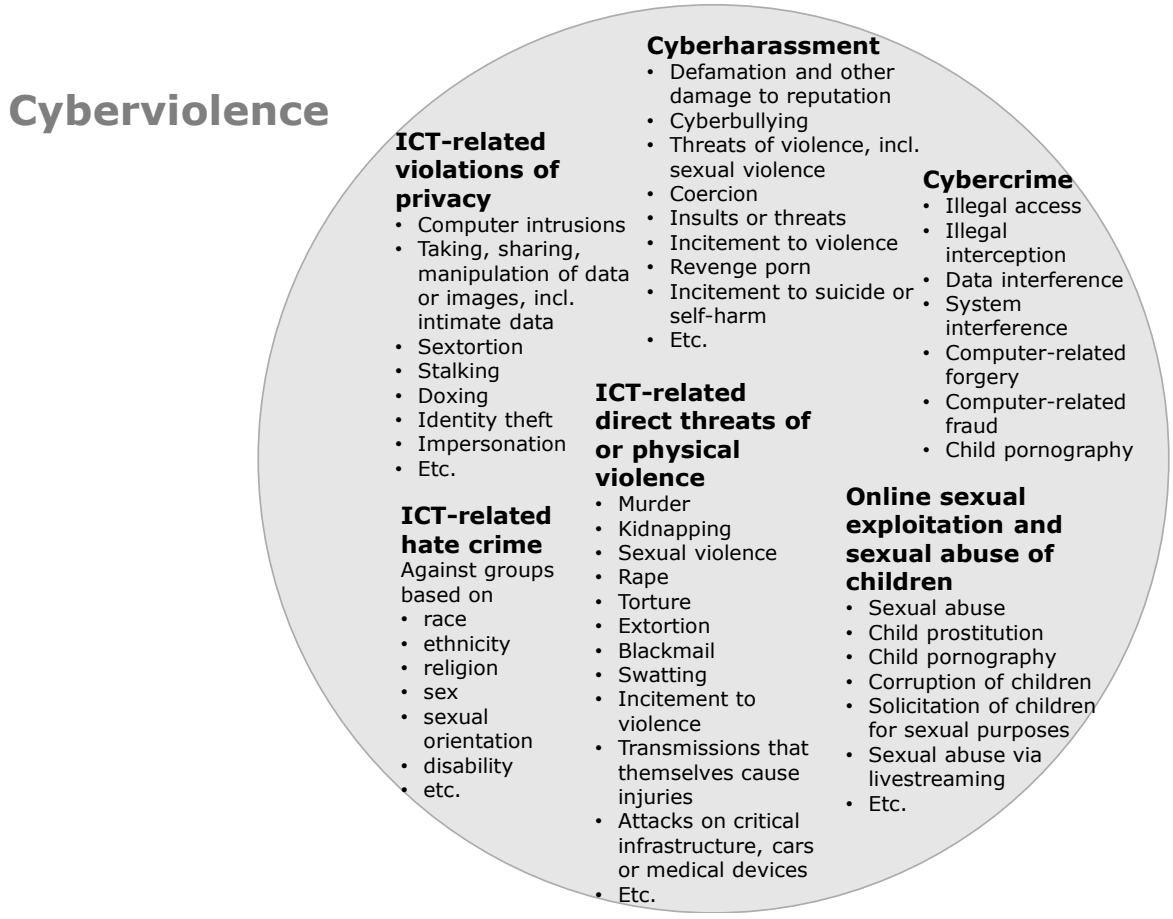
Laws on cybercrime may in particular be applied when violence such as injury or death is caused, for example, through computer-based attacks against critical infrastructure or medical devices.

2.1.2 Types of cyberviolence

In practice, acts of cyberviolence may involve different types of harassment, violation of privacy, sexual abuse and sexual exploitation and bias offences against social groups or communities. Cyberviolence may also involve direct threats or physical violence as well as different forms of cybercrime.

There is not yet a stable lexicon or typology of offences considered to be cyberviolence, and many of the examples of types of cyberviolence are interconnected or overlapping or consist of a combination of acts.

Not all of forms or instances of cyberviolence are equally severe and not all of them necessarily require a criminal law solution but may be addressed by a graded approach and a combination of preventive, educational, protective and other measures.



2.1.2.1 Cyberharassment

Cyberharassment is perhaps the broadest form of cyberviolence and involves a persistent and repeated course of conduct targeted at a specific person that is designed to and that causes severe emotional distress and often the fear of physical harm.

Cyberharassment is often accomplished by a "storm of abuse". Harassers terrorize victims by threatening violence. Offenders post defamatory falsehoods to cause the victim embarrassment or worse among friends, family or co-workers. Offenders impersonate victims in online ads, and suggest – falsely – that their victims are interested in sex with strangers. Sometimes, harassers

manipulate search engines to ensure the prominence of the lies in searches of victims' names. Harassers invade victims' privacy by posting their sensitive information, such as nude images or national identity numbers. Or harassers may use technology to knock people offline. [6] Cyberharassment in popular discourse may be described as or related to "revenge porn" or "sextortion."

Cyberharassment is often targeted at women and girls and termed "cyber violence against women and girls" (CVAWG or Cyber VAWG) involving:

- Unwanted sexually explicit emails or other messages;
- Offensive advances in social media and other platforms;
- Threat of physical or sexual violence;
- Hate speech meaning language that denigrates, insults, threatens or targets an individual based on her identity (gender) and/or other traits (such as sexual orientation or disability).[7]

Cyberharrassment thus involves a range of conduct, including for example "cyberbullying" and "revenge porn".

2.1.2.1.1 Cyberbullying

Cyberbullying is a form of cyberharassment that tends to be associated with victims who are children, often of high school age, while phenomena such as cyberstalking, sextortion or "revenge porn" are more likely to be associated with adults or young adults. The boundaries between these are not distinct and there is no common agreement on when to use which terms. Not all forms of cyberbullying necessarily constitute a criminal offence.

The literature identifies different types of cyberbullying which include cyberstalking, denigration, participation in exclusion/gossip groups, falsification of identity to post content online\flaming, harassment, impersonation, "outing", phishing, "sexting" and trickery [8]. As noted by some authors[9], cyberbullying can be considered as an umbrella for many online bullying activities some of which are more severe than others and have led to sexual manipulation, non-consensual creation and distribution of intimate images or videos, extortion, self-harm ("cutting") and suicide.[10] For this reason, from a criminal investigation and prosecution perspective, it is essential to distinguish between the different types of cyberbullying and it is also important to distinguish between the different roles individuals play in a given act of cyberbullying.

Cyberbullying is defined on the "Children's Rights" website of the Council of Europe[11] as using electronic technologies in order to bully another person through the Internet. It takes different forms. Examples of cyberbullying include nasty text messages or emails, rumours sent by email or

[6] See CITRON, DANIELLE K. *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, 2.
See also "the Disturbing Rise of Cyberattacks against Abortion Clinics" in WIRED (10 May 2017) https://www.wired.com/story/cyberattacks-against-abortion-clinics/
[7] http://eige.europa.eu/rdc/eige-publications/cyber-violence-against-women-and-girls
[8] See NOTAR, CHARLES E.; PADGETT, SHARON; RODEN, JESSICA. *Cyberbullying: Resources for Intervention and Prevention*. Universal Journal of Educational Research 1(3): 133-145, 2013.
[9] See EL ASAM, AIMAN; SAMARA, MUTHANNA. *Cyberbullying and the law: A review of psychological and legal challenge*. Computers in Human Behavior 65 (2016) 127-141.
[10] A recent example of cyberviolence is the "Blue Whale" challenge, which is structured along the lines of a video game where participants are awarded points. Children subscribe on a web page in order to be contacted by a "curator", who will establish 50 tasks that must be accomplished in the following 50 days. These tasks include many activities, such as watching video with extremely violent content or taking selfies in particularly dangerous situations (e.g. on the top of a building or close to railways or highways) but also extend to self-injury with sharp objects. The last task is to commit suicide. The Blue Whale challenge seems to be similar to "grooming" (see below); however, "grooming" is typically associated in criminal law with sexual activity and "Blue Whale" centres on "cutting" and self-harm.
[11] See http://www.coe.int/en/web/children/bullying (link last checked on April 3rd 2017).

posted on social networking sites, and embarrassing pictures, videos or websites. Cyberbullying typically involves a sustained series of such messages, whether orchestrated by a single person or a group of peers and the cumulative impact can be quite devastating.

Different authors have provided different definitions of cyberbullying that can be considered broadly as "any behavior performed through electronic or digital media by individuals or groups that repeatedly communicate hostile or aggressive messages intended to inflict harm or discomfort on others".[12]

Given the increasing number of victims among young people but also adults – and given that cyberbullying in extreme cases may lead to suicides[13] – one sees increasing research on and regulatory responses to this form of cyberviolence.

Victims of cyberbullying include journalists. A recent Council of Europe study on "journalists under pressure" [14] showed that journalists in more than half of the 47 member States have experienced cyberbullying during the last three years. Cyberbullying thus also impacts the freedom of expression.

The literature often associates cyberbullying with social media like YouTube, Facebook, Tumblr, Twitter, Instagram, Snap Chat, WhatsApp and chatrooms. By means of these media one can easily send threatening messages, offensive audiovisual materials or online "insult" to people. There are many examples of such behaviour: grooming, sexting, trolling and identity hacking.

The scientific literature identifies four elements which characterize cyberbullying and distinguish it from harmless forms of online behaviour such as cyber teasing or cyber arguing[15]. These criteria are the following:

- Intent to hurt - The perpetrator has the intention to hurt the victim by causing him or her intentional loss of reputation in the society and/or at work and/or destroy his/her family relations or inflicting other damage**.**

- Imbalance in power – In physical world bullying the perpetrator usually has a social interaction with the victim in which the perpetrator is physically and/or mentally stronger either in actual size, physical prowess, or social esteem. Typically for cyberbullying, a power imbalance occurs that arises either because of peer group pressure leading to social ostracism and isolation (in one form of the phenomenon) or because of an anonymous perpetrator (in another form of the phenomenon). Both

[12] See TOKUNAGA, Robert S. *Following you home from school: A critical review and synthesis of research on cyberbullying victimization*. Computers in Human Behavior, 26(3), 278.
For other definitions see:
See VAN LEEUWEN, J.C. Literature review on the research on cyberbullying definitions. Universiteit Twente. (2012). MOORE, Michael J.; NAKANO Tadashi; ENOMOTO Akihiro; SUDA Tatsuya. *Anonymity and Roles Associated with Aggressive Posts in an Online Forum*. 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. Published on http://www.cyberbullying.ca/ (link last checked 5th of April 2017).
SMITH, Peter K.; MAHDAVI Jess; CARVALHO Manuel; FISHER Sonja; RUSSELL Shanette; TIPPETT Neil. *Cyberbullying: its nature and impact in secondary school pupils*. 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. *Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools.* New Media & Society. Vol. 12(1). (2009), 109-125.
[13] For an overview of some well-publicised cases see *The Top Six Unforgettable CyberBullying Cases Ever* published on https://nobullying.com/six-unforgettable-cyber-bullying-cases/ (link last checked on 3rd of April 2017).
[14] Clark, Marilyn/Grech, Anna (2017): Journalists under Pressure. Unwarranted interference, fear and self-censorship in Europe. Council of Europe Publishing. Strasbourg.
[15] Cyber teasing or cyber arguing refers to the behaviour of sending messages that are not intended to harm another person, are not necessarily repetitive, and are performed in an equal power relationship.

forms amplify the imbalance of poser due to the wide reach of messages on social media, as well as by the fact that posted messages are hard to take down completely from the Internet. The Internet enables people – including those who know each other in person – to do or say things online that they would never do or say in direct contact. This is called the "disinhibition effect" of digital media.

- Recurrent behaviour and an ongoing process in which the victim is repeatedly abused - This can be taken literally by posting consecutive messages or follows from the fact that the posted messages can be shared, re-posted and may remain online indefinitely.

- Non-consensual distribution of intimate images – Perpetrators of this type of offense often target young people and adult women, but also minorities and other vulnerable groups. In fact, while on the one hand the availability of several devices able to create and exchange intimate images is has given rise to an emerging market of user generated pornographic content which some have regarded as empowering[16]. On the other hand the production and exchange of sexually explicit images can be used for criminal activities such as online stalking or cyberstalking, sextortion, "revenge porn", sexchatting[17] and grooming that fit into the general category of cyberharassment and are mainly targeted at women and girls.

2.1.2.1.2 "Revenge porn"[18]

"Revenge porn" is a term in popular discourse that centres on the sexually explicit portrayal of one or more persons that is distributed without the subject's consent. The phenomenon predominantly involves a partner in an intimate relationship disseminating the material in order to humiliate or intimidate the victim. The phenomenon, emerged as early as the 1980s (being a regular feature in *Hustler* magazine) and was linked to "amateur pornography", before transforming into sexually explicit videos disseminated over the Internet (such as the amateur porn aggregator Xtube in 2008).[19] "Revenge porn" is a crime that has been recognised by several regulations at local and national levels and has involved civil suits and criminal offences in various countries, although not always in the same manner. One legal formulation criminalises the unlawful (meaning non-consensual) disclosure, distribution, dissemination or promotion of intimate images or videos.

In the USA, 35 States and the District of Columbia have adopted laws prosecuting revenge porn crimes,[20] while in Europe and other countries the situation is more fragmented or less regulated.

Canada amended its Criminal Code (section 162.1) in March 2014 to prohibit the non-consensual distribution of intimate images (it came into force in March 2015). A companion provision (section 162.2, amended in 2015) empowers a court to order the removal of intimate images from the Internet; permits the court to order forfeiture of the computer, cell phone or other device used in the offence; provides for reimbursement to victims for costs incurred in removing the intimate

[16] See PAASONEN, Sussanna. *Labors of love: netporn, Web 2.0 and the meanings of amateurism*. New Media & Society 12(8) 1297–1312.
[17] Sexchatting can be defined as "[…] the casual exchange of vernacular views about sexual beliefs, rumours and behavior, conducted either synchronously or asynchronously". In the case of the internet based sex chat, the communication can happen in a monitored or unmonitored environment set by the webmaster. See ERNI, John Nguyet. *Sex/Text: Internet Sex Chatting and "Vernacular Masculinity" in Hong Kong*. International Proceedings of Economics Development and Research, Vol. 44, 56-60.
[18] It is not recommended to use this term in relation to the sexual exploitation and sexual abuse of children. http://luxembourgguidelines.org/english-version/
The term "image-based sexual abuse" may be used as an alternative.
[19] In 2010 the site *IsAnyoneUp* was launched: it often provided the subject's identifying information in the videos. The owner of the site, Hunter Moore, pled guilty to identity theft and hacking in 2015. Kevin Bollaert, who ran the revenge porn site *UGotPosted*, was charged in the USA with 31 counts, including extortion and identity theft, and sentenced in 2015 to 18 years in prison. In 2014, an Ohio decision against him awarded damages of $385,000 on behalf of a minor depicted in photos. Other cases have been charged in the United Kingdom in recent years.
[20] https://www.cybercivilrights.org/revenge-porn-laws/

image from the Internet or elsewhere; and empowers the court to make an order to prevent someone from distributing intimate images.

In Germany in May 2014, a court ruled that intimate photographs of partners should be deleted if a partner calls for it. The decision by the German Higher Regional Court of Koblenz came after a divorced man refused to delete erotic images of his former wife following their split. He was taken to court by his former wife, who won her case and saw the pictures deleted.[21]

In France, article 67 of Law n° 2016-1321 of 7 Octobre 2016 "pour une République numérique" states that:

> 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.[22]

In 2015, the UK amended the Criminal Justice and Courts Act 2015 including under the "Offences involving intent to cause distress" the crime of "Disclosing private sexual photographs and films with intent to cause distress."[23]

2.1.2.2 ICT-related violations of privacy

Many forms of cyberviolence represent or are related to a violation of victims' privacy.[24] This may include computer intrusions to obtain, steal, reveal or manipulate intimate data, the researching and broadcasting of personal data ("doxing"), or acts such as "cyberstalking" or "sextortion/revenge porn".

2.1.2.2.1 Cyberstalking

Cyberstalking "[…] refers to stalking in an electronic format. With the anonymity, ease, and efficiency of the Internet, cyberstalking can occur in a multitude of ways. Cyber stalkers can use personal information about the victim to threaten or intimidate the victim. Cyberstalkers can also send unwanted, repetitious emails or instant messages that may be hostile threatening in nature. Cyber stalkers can also impersonate their victims online by stealing login information for an email account or social networking page and posting messages on other peers' pages". [25]

"Stalking encompasses a pattern of repeated, intrusive behaviors – such as following, harassing, and threatening – that cause fear in victims".[26] In recent years, this phenomenon increasingly involved the use of mobile technologies (such as smartphones) as well as computers, laptops, tablets, and digital cameras. Such stalking predominantly takes the form of men victimizing women:

---

[21] https://www.thelocal.de/20140522/court-forces-ex-lovers-to-delete-sexy-photos
[22] https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=3271AC8D94E47247A2CFDC0389186E84.tpdila17v_1?idArticle=JORFARTI000033203291&cidTexte=JORFTEXT000033202746&dateTexte=29990101&categorieLien=id
[23] http://www.legislation.gov.uk/ukpga/2015/2/section/33
[24] For the ease of tracing the location of persons see for example https://www.wired.com/story/track-location-with-mobile-ads-1000-dollars-study/
[25] See 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, Issue 1, 48.
[26] 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)

> Contrary to popular misconceptions, research shows that the majority of stalking is perpetrated not by strangers or acquaintances but by intimate partners or ex-partners … Evidence demonstrates that men are the main perpetrators of intimate partner stalking, both in Australia and internationally …. Reviews of international research demonstrate that women are more likely to be stalked than men … and are more likely to experience fear due to stalking.[27]

Research indicates that cyberstalking by intimate partners often occurs in the context of domestic violence and is a form of *coercive control*.[28] Stalking by intimate partners can be persistent and dangerous. Woodlock cites a national U.S. survey that "found that cases involving intimate partners lasted 2.2 years on average, compared with 1.1 years for stalking by others" and has been strongly associated with homicides and attempted homicides. ICTs are used not only to keep the victim under surveillance (hidden digital cameras, GPS tracking of vehicles) but include harassment and control through persistent emails and constant texting (SMS). Behaviour that in other contexts is conducted consensually for pleasure, such as "sexting", is used coercively and non-consensually to control, harass or shame by intimate partners engaged in cyberstalking.[29]

2.1.2.2.2 Sextortion

Sextortion is a term in popular discourse that encompasses activities that (a) involve manipulation or coercion to perform sexual activities for the benefit of the aggressor and/or to create sexually explicit images of the victim and (b) the traditional crime of extortion. Although the crime may include the threat to disseminate such images or videos once they have been created, it is just as common that the coercion may involve the threat to hurt the victim's family or friends if sexual activity is not undertaken and recorded or transmitted to the aggressor. The aggressor's motivation may also be revenge, humiliation or monetary gain. It is often carried out remotely over computer networks and may involve recording images or live streaming video (i.e., using a Web cam). Perpetrators are often current, former or would-be romantic or sexual partners.[30] There are cases of sextortion, however, where the perpetrator is a stranger and a serial aggressor with victims in dozens of countries. Offenders often use a variety of computer skills including hacking, creation of multiple false identities on social media sites, interception of private communications and so forth. In this regard, sextortion has been a component of the more severe forms of cyberbullying and has also been an element in some forms of cyberstalking and cyber harassment. "Sextortion" often entails the non-consensual distribution of intimate images, even if that distribution is only between the offender and the victim, rather than broad dissemination.

[27] Woodlock 2016: 584-585

[28] Woodlock (2016: 585) states: "Coercive control is a theoretical framework that encompasses physical abuse that occurs in domestic violence, but which also includes tactics not traditionally viewed as serious forms of abuse. These tactics include strategies to control and intimidate, such as isolation, surveillance, threats of violence, micromanagement of daily activities (e.g., regulation of showering and eating) and shaming (Stark 2007). The theory of coercive control also encompasses the effects on the victims of these tactics. Stark (2012) believes these effects have more in common with the experiences of hostages and the victims of kidnappings than of victims of conventional assaults. Stark acknowledges that although women can be abusive in intimate relationships, men are the main perpetrators of coercive control because it is a form of violence rooted in systemic inequality, which affords men a sex-based privilege. Stark views this sex-based privilege as the essence of coercive control, where male offenders 'exploit persistent sexual inequalities in the economy and in how roles and responsibilities are designated in the home and the community to establish a formal regime of domination/subordination behind which they can protect and extend their privilege'(p.206)."

[29] Woodlock 2016: 587-588.
ICT-facilitated stalking can thus be associated with the phenomenon which the internet and media dubbed "revenge-porn" which often involves public humiliation of the victim.

[30] See https://www.wearethorn.org/sextortion/1880/ (link last checked 4th of April 2017).

2.1.2.3 Online sexual exploitation and sexual abuse of children[31]

Children seem to represent a primary group of victims of cyberviolence, in particular with respect to online sexual violence.

While the "online sexual exploitation and sexual abuse of children" are not necessarily new and distinct forms of sexual exploitation and sexual abuse of children, ICTs have increased the accessibility to children by persons looking to sexually abuse and exploit them. ICTs facilitate the sharing of images and videos of the sexual abuse and thus reinforce the long-lasting harmful impact of the abuse of children. ICTs also contribute to making commercial gains from sexual exploitation of children easier. ICTs however do not, in and by themselves, give rise to distinct types of sexual offences against children.

Online sexual exploitation and sexual abuse of children includes the behaviour listed in articles 18 to 23 of the Lanzarote Convention[32] and in article 9 of the Budapest Convention in an online environment or otherwise involving computer systems:

- Sexual abuse (article 18), that is, "a) engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities; or b) engaging in sexual activities with a child where:
  - use is made of coercion, force or threats; or
  - abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or
  - abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence."

- Child prostitution (article 19), that is, "a) recruiting a child into prostitution or causing a child to participate in prostitution; b) coercing a child into prostitution or profiting from or otherwise exploiting a child for such purposes; or c) having recourse to child prostitution."

- Child pornography (article 20), that is, "a) producing child pornography; b) offering or making available child pornography; c) distributing or transmitting child pornography; d) procuring child pornography for oneself or for another person; e) possessing child pornography; f) knowingly obtaining access, through information and communication technologies, to child pornography". "Child pornography" shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes.[33]

- Corruption of children (article 22), that is, "the intentional causing, for sexual purposes, of a child who has not reached the age [below which it is prohibited to engage in sexual activities with a child] to witness sexual abuse or sexual activities, even without having to participate".

[31] The replies by Mexico suggests that the concept be extended to cover "other dependent persons" such as persons with disabilities.
[32] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/201
[33] See also Article 9 Budapest Convention.
While the term "child pornography" is used in international instruments (including the Budapest and Lanzarote Conventions) and the domestic laws of many countries, the term and concept have also been contested. See, for example, https://www.interpol.int/News-and-media/News/2018/N2018-010.
Thus, while it cannot be ignored that the term "child pornography" denotes a specific offence and is the basis for criminal justice action in a large number of countries, this concept has limitations and should be used with caution.

- "Solicitation of children for sexual purposes" (article 23) – also called "grooming" – that is, "the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set [below which it is prohibited to engage in sexual activities with a child] for the purpose of committing any of the offences established in accordance with article 18, paragraph 1.a [engaging in sexual activity with a child], or article 20, paragraph 1.a [producing child pornography], against him or her, where this proposal has been followed by material acts leading to such a meeting".

Online sexual exploitation and sexual abuse are major forms of cyberviolence targeting children. It should be kept in mind, however, that children are also victims of other types of cyberviolence. A useful mapping can be drawn from the "Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children".[34] Building upon previous analyses, including the EU Safer Internet Project, the study suggests the following areas:

- "Child sexual abuse material";
- "Commercial sexual exploitation of children";
- "Cyberenticement, solicitation and online grooming of children";
- "Cyberbullying, stalking and harassment"; and
- "Exposure to harmful content".

2.1.2.4 ICT-related hate crime

Cyberviolence may be motivated by "a bias against the perceived personal characteristic of the victim or a perceived group membership of the victim. These groups or characteristics include but are not limited to race, ethnicity, religion, sexual orientation or disability." [35]

It includes conduct that can be criminalised under the Budapest Convention's Additional Protocol on Xenophobia and Racism (ETS 189).

Hate crime has serious consequences for individuals and societies and may lead to communal violence and the destabilisation of entire societies.

The Group concluded, however, that a full mapping of the issue of hate crime would not be feasible within the mandate and timeframe given by the T-CY.

2.1.2.5 ICT-related direct threats or actual violence

Cyberviolence also comprises direct threats of violence or direct physical violence. Computer systems may be used in connection to murder, kidnapping, rape and other acts of sexual violence, or extortion.

Forms of direct violence include interference with medical devices causing injuries or death,[36] or attacks against critical infrastructure by means of computers. "Swatting" is another example.

[34] (UNODC 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.pdf
In the UK, for example, the police and the Crown Prosecution Service "have agreed the following definition for identifying and flagging hate crimes: Any criminal offence which is perceived by the victim or any other person, to be motivated by hostility or prejudice, based on a person's disability or perceived disability; race or perceived race; or religion or perceived religion; or sexual orientation or perceived sexual orientation or a person who is transgender or perceived to be transgender."
https://www.cps.gov.uk/hate-crime
[36] https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

2.1.2.5.1 Swatting

"Swatting" is an example of how computer systems can be misused for many types of conduct with violent impact on victims. It is the use of telephones and often computer systems to deceive an emergency service in order to send law enforcement to a specific location based on a false report. The name comes from the acronym "S.W.A.T." (Special Weapons and Tactics) which are law enforcement units that have specialized training and may employ military-style equipment. False reports include reporting homicides in someone else's home, bomb threats, and kidnapping. "Swatting" may fall under a variety of criminal statutes such as uttering death threats, conspiracy to commit device fraud, obstruction of justice, and public mischief. These are not merely prank phone calls: perpetrators typically use caller ID spoofing and social engineering and some demonstrate the sophisticated use of computer systems and software to make it appear calls are coming from different locations (sometimes in different countries from the offender's point of origin). [37] Swatting may be terrifying and dangerous to the victims, who have been killed by responding law enforcement or who have suffered physical injuries such as bullet wounds and heart attacks.[38]

2.1.2.6 Cybercrime

Considering the definition proposed above, some forms of cybercrime may also be considered acts of cyberviolence, such as illegal access to intimate personal data, the destruction of data, blocking access to a computer system or data, etc. This is for example captured in 18 United States Code Section 1030(a)(7) on "extortion involving computers".

Denial of service attacks may lead to physical harm of individuals – for example, if fire emergency telephone lines are unable to accept calls or if traffic control systems or hospital services are disabled.

2.2 Statistics

An increasing number of studies – many of them with statistical data – is available covering different aspects of cyberviolence, in particular targeting children, as the following examples illustrate.

Given that concepts and definitions are yet to be agreed upon, and that cyberviolence is often a continuum of offline violence, it is difficult to compare different sets of data and to arrive at an overall assessment of the scale and impact of cyberviolence.

Nevertheless it is safe to conclude that cyberviolence is a growing problem with significant impact on an increasing number of individuals, in particular women and children, in many regions of the world.

[37] In 2009, blind phreaker Matthew Weigman received a sentence of 11 years in prison in the United States for swatting. In 2014 in British Columbia, Canada, a teenager using the handle "Obnoxious" committed 40 attempted or successful acts of swatting in several countries. He pled guilty to 23 charges.
[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
For a recent case (December 2017) with fatal consequences see http://www.nydailynews.com/news/national/unarmed-kan-man-killed-cops-victim-swatting-prank-article-1.3726171
According to this report, the FBI estimates that there are some 400 swatting cases per year in the USA.

2.2.1 Data on cyberviolence against children

2.2.1.1 Cyberbullying

A research project carried out between July and October 2016 shows that, from a nationally-representative sample of 5,700 students between the ages of 12 and 17 in the USA, 33.8% of the students were victims of cyberbullying[39] such as by mean or hurtful comments online (22.5%), online rumours (20.1%), posting of mean or sexual comments (12.7%), online threats to hurt (11.9%), posting of mean or hurtful pictures (11.1%), impersonation (10.3%), or mean comments about race or colour (10.1%).

While bullying is not a new phenomenon, the availability of social media, applications and mobile devices with in-built cameras favour the spreading of cyberbullying.[40] Both males and females are victims, but offenders are more often males in the USA.[41]

A survey published by Vodafone in September 2015[42] shows how cyberbullying is perceived in eleven countries (Czech Republic, Germany, Greece, Ireland, Italy, Netherlands, New Zealand, South Africa, Spain, UK and USA). Children between 13 and 18 years of age have been most often bullied in New Zealand (30%), followed by the USA (27%) and Ireland (26%), while children in the Czech Republic (8%), Spain (8%) and Italy (11%) have been least often bullied.

Cyberbullying is an important issue also in Asian countries. For example, in Malaysia, a website[43] reports that:

- 33% of Malaysian children have been bullied online;
- 15% have committed cyberbullying acts;
- 27% of Malaysian parents warn their kids about the risks of using the Internet, but only 18% educate their children about online etiquette.

A 2014 DiGi CyberSafe study,[44] using a sample of 14,000 school children in Malaysia, showed that:

- approximately 26% of Malaysian children have experienced Internet bullying, with 13-15-year-olds being the most common targets;
- the level of online harassment rose to 70% with name calling and posting of inappropriate messages or photos on social media being the most common offenses;
- at the same time, 64% of young people didn't consider sending improper SMSes, posting inappropriate photos, and pretending to be someone else to be online bullying offenses;
- 40% of children surveyed said they wouldn't know how to handle bullying or protect themselves online;
- two thirds of children 13 years and younger took few to no protective measures when going online; yet 53% of them believed they could navigate the Internet safely;
- approximately 70% of children under 13 showed little concern over invasion of their privacy or knowing who they interact with online;
- over 40% of kids who considered online safety important exercised low levels of online protection.

[39] See http://cyberbullying.org/2015-data (link checked last on 3rd of April 2017).
[40] For some statistics on cyberbullying and social media see http://www.meganmeierfoundation.org/cyberbullying-social-media.html (link checked last 3rd of April 2017).
[41] See http://cyberbullying.org/2015-data (link checked last on 3rd of April 2017).
[42] http://www.vodafone.com/content/index/media/vodafone-group-releases/2015/groudbreaking_global_survey.html
[43] See https://nobullying.com/bullying-in-malaysia-2/ (link checked last 26th of July 2017).
[44] http://www.digi.com.my/aboutus/media/press_release_detail.do?id=8600&page=1&year=2014

A survey[45] by Stairway Foundation Inc. showed that in the Philippines, from a sample of 1,268 children aged 7 to 12 and 1,143 children aged 13 to 16:

- 80% of teenagers between 13 to 16 years are cyberbullied through social media, while 60% of their counterparts between 7 and 12 years old suffered the same abuse;
- 30% of children aged 7 to 12 were bullied through threats and 10% were humiliated or had their private conversations exposed;
- 30% of teenagers aged 13 to 16 were bullied through photo editing;
- The survey also shows that, for both groups, 20% of the cyberbullies are people using fake profiles online.

These and other studies indicate that children are disproportionately affected by cyberviolence in the form of cyberbullying.

2.2.1.2 Online sexual violence against children

Numerous reports are available underlining the scale of online sexual violence against children.

For example, in 2016, according to the 2016 Annual Report of the United Kingdom's Internet Watch Foundation[46] – based on reports received from 16 portals around the world:

- the number of domains hosting child sexual abuse imagery increased from 1,991 in 2015 to 2,415 in 2016, that is, by 21%;
- 57,335 out of 102,932 URLs reported contained child sexual abuse imagery;
- 455 newsgroups were confirmed as containing child sexual abuse imagery;
- 53% of children represented in images were assessed as aged 10 or younger.

The scale of online child sexual violence is also reflected in law enforcement operations. For example, the takedown of Playpen – one of the world's largest child sexual abuse websites with more than 150,000 users worldwide - and the subsequent "Operation Pacifier" led to the arrest of 368 suspected child sex abusers in Europe while the lead administrator of Playpen was sentenced to 30 years imprisonment in the USA in May 2017.[47]

INTERPOL reports that 10,000 victims of child sexual abuse have been identified through its International Child Sexual Exploitation (ICSE) database. [48]

There is thus no doubt that children are disproportionately affected by online sexual violence.

2.2.2 Data on cyberviolence against women

While the issue of cyberbullying involving children is well researched, statistical studies focusing on cyberviolence against women in different regions of the world may be less prevalent.

The 2015 report of the United Nations Department of Economic and Social Affairs, "The World's Women 2015, Trends and Statistics," [49] notes that "1 in 3 women have experienced physical/sexual violence at some point in their lives," but data on the role of ICT – with the exception of a brief reference to mobile phones and social media – is missing.

[45] See "*Cybersafe survey 2015*" http://www.cybersafe.asia/wp-content/uploads/2016/03/Cybersafe-Survey_LOWRES.pdf (checked last 26th of July 2017).
[46] https://www.iwf.org.uk/sites/default/files/reports/2017-04/iwf_report_2016.pdf
[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

The EU Fundamental Rights Agency (FRA) in 2014 published a detailed survey on "Violence against women: an EU-wide survey".[50] According to this survey, in the twelve months prior to the survey:

- some 7% of women aged 18-74 (that is, 13 million women in the 28 EU member States) had experienced physical violence;
- some 2% (3.7 million) had experienced sexual violence;
- some 5% (9 million) had experienced situations "where the same person had been repeatedly offensive or threatening" towards them with respect to a list of different actions; for example, the same person has repeatedly "Loitered or waited for you outside your home, workplace or school without a legitimate reason;" or "Made offensive, threatening or silent phone calls to you";
- some 5% (9 million) – including 11% in the age group 18 to 29 – had experienced "forms of sexual cyberharassment … including unwanted sexually explicit emails or SMS messages that were offensive". Some 11% (more than 20 million) had experienced cyberharassment since the age of 15;
- some 5% (9 million) had experienced stalking, and from among these 23% "had to change their email address or phone number in response to the most serious case of stalking."

A 2017 report[51] of the Pew Research Center on online harassment in the USA found that, from a sample of 4,248 adults:

- 41% of Americans have been personally subjected to harassing behaviour online, and an even larger share (66%) has witnessed such behaviour directed at others;
- nearly 18% have been subjected to particularly severe forms of harassment online, such as physical threats, harassment over a sustained period, sexual harassment or stalking;
- social media platforms are an especially fertile ground for online harassment that usually targets a personal or physical characteristic, that is, 14% of Americans say they have been harassed online specifically because of their political views, while roughly 9% have been targeted due to their physical appearance and 8% for their race or ethnicity or gender;
- overall, men are somewhat more likely to experience some form of harassing behavior online but women – and especially young women – encounter higher rates of sexualized forms of abuse. Some 21% of women aged 18 to 29 report having been sexually harassed online. In addition, roughly half (53%) of young women aged 18 to 29 say that someone has sent them explicit images they did not ask for.[52]

A 2016 report on cyberviolence against women and minorities in India[53] states that:

- from among 500 people (97% of whom were women) surveyed, 58% reported having faced some kind of online aggression in the form of trolling, bullying, abuse or harassment;
- 36% of respondents who had experienced harassment online took no action at all. 38% reported that they had intentionally reduced their online presence after suffering online abuse;

[50] http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report
[51] See 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 (site checked last 26th of July)
[52] See Pew Research Center, July, 2017, "*Online Harassment 2017*", p. 7.
[53] See the report "'*Violence' Online in India: Cybercrimes Against Women & Minorities on Social Media*" https://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf

- women found it difficult to think of online harassment as being on par with violence, even though 30% of those who had experienced it found it "extremely upsetting" and 15% reported that it leads to mental health issues like depression, stress, and insomnia;
- only a third of respondents had reported harassment to law enforcement; among them, 38% characterized the response as "not at all helpful."

A report on "Women's Rights Online" of 2015[54] – covering nine cities in Africa and Asia – identified online harassment as one of the constraints limiting the use of technology by women. According to the study:

- "overall, reported experience of harassment and abuse was low. Only around 13% of women (and 18% of men) said they had experienced such incidents via phone call or text message, while 13% of women and 11% of men who use the Internet had suffered abuse via emails or social media posts";
- however, in some cities, a large share of women but also men experienced "personal bullying (including harassment or stalking)" during the past two years when using mobile phones (e.g. 28% of women in Jakarta, 21% of women in Kampala, 60% of men in Nairobi) or the Internet (45% of women in Kampala, 21% of women and 19% of men in Nairobi).

According to a Women's Aid survey from 2017 :

- 45% of domestic violence victims reported experiencing some form of abuse online during their relationship;
- 48% reported experiencing harassment or abuse online from their ex-partner once they'd left the relationship. 38% reported online stalking once they'd left the relationship;
- 75% reported concerns that the police did not know how best to respond to online abuse or harassment. This includes 12% who had reported abuse to the police and had not been helped[55].

2.3 Challenges to the investigation and prosecution of cyberviolence

A range of issues arises in relation to cyberviolence that need to be taken into consideration. For example:

- Victims have no information on available remedies:
  A particularly-distressing aspect of cyberviolence is that victims may not know how to get help. They may be warned viciously not to contact law enforcement, and they may not know whom to contact anyway (see further discussion below). Their normal methods of communication may be cut off or compromised and a sustained attack may so shock and disturb them that their ability to defend themselves, or even to think straight, may be diminished.[56]

[54] http://webfoundation.org/docs/2015/10/womens-rights-online21102015.pdf
[55] Clare Laxton, Women's Aid, Virtual World, Real Fear, Women's Aid report into online abuse, harassment and stalking, 2014, available online at 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

- Limited help by law enforcement:
  Victims may have the impression that law enforcement was of little use, or that it required great persistence to obtain useful aid. Cyberviolence may involve methods that are particularly difficult for police forces to investigate, and victims may be told – correctly or incorrectly – that there is nothing that law enforcement can do. Like any other form of violence against women, online violence against women is often overlooked because of a lack of awareness and gendered understanding of violence. Victims' experience are often considered as "incidents" rather than patterns of behaviour, and victims are blamed for the violence they face. And thus, a single individual's complaint may fail to reveal that it is part of a larger pattern in which a particular perpetrator may be targeting dozens of victims in multiple jurisdictions, such as was the case with Aydin Coban who victimized more than three dozen teenage girls and boys in many countries including the Netherlands and Canada (leading to the suicide of 15 year-old Amanda Todd).[57] In some countries, only certain police forces have authority to investigate such crimes. It may be difficult for victims to learn which unit to turn to or, as a practical matter, it may be difficult to work with the unit (if the unit is in the capital and the victim is hundreds of kilometres away). Victims may also encounter law enforcement or officials who are unacquainted with the phenomenon and do not understand the potential gravity. Finally, local law may not address certain types of attack under criminal law (possibly for valid reasons), so there is simply no legal basis for prosecution.[58]

- Protection of children versus protection of adult victims:
  Children may to some extent be better protected than adults because child exploitation statutes may be usable to cover cyberviolence against children. If a 14-year-old girl is

[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," July 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, slate.com, "English Police Apologize to a Woman Who Reported Her Stalker 125 Times Before He Stabbed Her," June 29, 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," April 12, 2017, http://www.hindustantimes.com/india-news/cop-victim-shames-minor-facing-harassment-on-social-media-maneka-intervenes/story-jF3bFnX1SL10f3UJci7ApJ.html; BAUM, KATRINA, et al, Bureau of Justice Statistics, U.S. Department of Justice Office of Justice Programs, "National Crime Victimization Survey Stalking Victimization 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 Against Women & Minorities on Social Media"* https://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf; INTER-PARLIAMENTARY UNION, "Sexism, harassment and violence against women parliamentarians," October 2016, https://ipu.org/resources/publications/reports/2016-10/sexism-harassment-and-violence-against-women-parliamentarians; CYBER CIVIL RIGHTS INITIATIVE, FAQs, "I'm being told that I should file a police report, what should I know before I do?," https://www.cybercivilrights.org/faqs-usvictims/; "Aren't victims protected by existing criminal laws against stalking, harassment, and voyeurism?," https://www.cybercivilrights.org/faqs/; 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,"* September 15, 2017, panel discussion: "Holding Offenders Accountable," http://www.law.umaryland.edu/about/news_details.html?news=2218; CHIARINI, Annmarie, keynote address at symposium, https://www.youtube.com/watch?v=G6cdN3TzDlo&index=4&list=PLYBWgedwTFEZq8RB1mOVc20zOmIhMd-Fi (links last checked November 11 and 13, 2017).
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

stalked and secretly filmed, for example, child exploitation statutes may be available for a prosecution. However, a country's statutes may not offer the same protection to a 19-year-old woman.[59]

- Role of social media providers:
  Various Internet/social media platforms can play a role in cyberviolence. Information on social media can be used to identify and locate victims, to learn about their vulnerabilities (what shifts they work and their commuting hours, for example), to gather details about them, and for other purposes. Other platforms may be used to post victimizing messages – solicitations for rape, for example – or to threaten targets.
  Of course, some platforms have fostering crime as a business model, so complaints and removal are irrelevant to them. Other platforms offer mechanisms for complaints or for removal of postings. These mechanisms may not be sufficient or quick enough, and victims may find that a posting has been disseminated widely and removal in one location is useless.
  In some countries, groups have begun to protest the lack of action by providers. There is an opportunity for Internet platforms, especially those with wide reach and sufficient staffing, to take active steps against cyberviolence, including removal of posts and preserving evidence.[60]
  In January 2018, it was reported that Facebook reached a settlement in Northern Ireland with a teenage victim of revenge porn "after her [intimate] photo appeared several times between November 2014 and January 2016. She alleged misuse of private information, negligence and breaching the Data Protection Act. Her lawyers [….] claimed the settlement had "moved the goalposts" in terms of how social media networks such as Facebook would have to respond to indecent and abusive messages and images being posted on their sites."[61]

- Free speech versus hate speech:
  Countries have different views about the degree to which speech should be limited by society – that is, where to set the balance between one person's fundamental right to express him/herself and another person's fundamental right to safety. For example, a website may post the schools that the children of police attend, with photos of the children. If no explicit threat is included on the site, countries may differ about whether such postings constitute illegal speech. If an explicit threat is included, countries may still differ about whether it is serious enough that it constitutes a crime.

  Many countries restrict or ban hate speech, normally defined as expression that attacks discrete identifiable groups, such as religious, ethnic, or national groups.

  The US does not restrict hate speech absent a sufficient level of danger. Given the current concentration of data subject to US law, US domestic law has much influence on the Internet. Its rejection of many restraints on speech has repercussions for people who are outside the United States. In addition, because of US law, the US government sometimes declines to provide mutual legal assistance in cases that involve hate speech.

  As private entities, providers are permitted under US law to make their own rules about what material they carry on their systems. Some choose to regulate content, but others

[59] There may be valid reasons for differentiating in criminal law between the level of protection granted to children and the protection granted to adults.
[60] See 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

permit speech that is illegal outside the US. In recent years, European countries have sought cooperative agreements with such providers to remove speech that is illegal by European standards. Some countries have taken binding steps to enforce such removal.

2.4 Cyberviolence against women and children as addressed by Istanbul and Lanzarote Conventions

The Budapest, Lanzarote and Istanbul Conventions require the criminalisation of specific conduct that includes or entails violence against women and children.

2.4.1 "Lanzarote" Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201)[62]

The Lanzarote Convention as a whole is aimed – through a holistic approach – at the protection of children against sexual violence. It covers:

- preventive measures such as the recruitment, training and awareness raising of persons working in contact with children (article 5), education for children (Article 6), preventive intervention programmes and measures (article 7), measures for the general public (article 8) and the participation of children, the private sector, media and civil society (article 9);
- protective measures and assistance to victims, including reporting suspicion of sexual exploitation or sexual abuse (article 12), helplines (article 13), assistance to victims (article 14);
- intervention programmes or measures;
- substantive criminal law, including
  - sexual abuse (article 18),
  - child prostitution (article 19),
  - child pornography (article 20),
  - participation of a child in pornographic performances (article 21),
  - corruption of children (article 22),
  - solicitation of children for sexual purposes (article 23);
- investigation, prosecution and procedural law, including measures to protect and respect the rights, interests and special needs of children during investigations and criminal proceedings;
- international cooperation.

The Convention establishes a monitoring mechanism which is in place since 2011 in the form of the "Lanzarote Committee".[63]

As Parties to the Lanzarote Convention encountered challenges with regard to the effective implementation of article 23 ("grooming"), on 17 June 2015, the Lanzarote Committee adopted an Opinion [64] on the solicitation of children for sexual purposes through information and communication technologies.

[62] http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680084822
[63] https://www.coe.int/en/web/children/lanzarote-committee
[64] See https://rm.coe.int/168064de98 (link checked on May 19th 2017).

The Opinion specifies the obligations imposed on the Parties by article 23, notably to criminalise the intentional proposal of an adult to meet a child for the purpose of committing illegal sexual acts against the child. This intentional proposal is organised and expressed through the means of information and communication technologies and has to be followed by material acts leading to such a meeting.

The Opinion reiterates that children may be exposed to some of the same risks online as offline, such as being persuaded to engage in real or simulated sexually explicit conduct, being recruited or coerced to participate in pornographic performances, or caused to witness sexual abuse or sexual activities, and that these types of unlawful conduct that may occur online are criminalised by other provisions of the Convention.[65]

The Opinion gives pointers to States wishing to go beyond the requirements and scope of article 23, in particular by proposing that they make grooming a criminal offence even in cases where solicitation does not result in a meeting in person but remains exclusively online. The Opinion also notes that responsibility for the investigation and prosecution of online grooming should remain with law enforcement authorities and the criminal justice system. When appropriate, assistance may be requested from specialised NGOs, but neither these nor the public should become de facto law enforcement agencies.

Furthermore, following adoption of the above opinion, the Lanzarote Committee set up a working group to examine links between sexual abuse and sexual exploitation and new technologies (such as sexting, "sextortion", live streaming of sexual abuse and other phenomena), and whether such phenomena were sufficiently covered by the Lanzarote Convention.

Based on the results of this working group, the Lanzarote Committee approved at its 18th plenary (10-12 May 2017) the "Interpretative Opinion on the Applicability of the Lanzarote Convention to sexual offences against children facilitated through the use of information and communication technologies (ICTs)".[66] Accordingly:

- The common understanding of the Lanzarote Committee is that the Lanzarote Convention establishes that Parties shall protect children against all forms of sexual exploitation and abuse, including those facilitated through the use of ICTs, even when the text of the Lanzarote Convention does not specifically mention ICTs. The existing offences in the Lanzarote Convention thus remain criminalised by national law in the same way, whether or not committed via ICTs.

- The Lanzarote Committee suggests that, "in implementing the Lanzarote Convention, Parties should ensure appropriate response to technological development and use all relevant tools, measures and strategies to effectively prevent and combat sexual offences against children, which are facilitated through the use of ICTs".

- Among the possible activities to undertake, the Lanzarote Committee suggests that Parties allocate resources to ensure effective investigation and prosecution of sexual offences against children facilitated through the use of ICTs and that training should be provided to authorities responsible for investigation and prosecution. In addition to this, the Parties shall encourage cooperation between competent state authorities, civil society and the private sector in order to better prevent and combat sexual abuse and exploitation of children facilitated through the use of ICTs.

[65] Namely, Articles 20§1, 21§1, 22 and 24§2 of the Convention.
[66] https://rm.coe.int/t-es-2017-03-en-final-interpretative-opinion/168071cb4f (link checked on 26th of July 2017)

The Lanzarote Committee then launched on 20 June 2017 the 2nd monitoring round for the Lanzarote Convention by circulating a thematic questionnaire on the "Protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs)". The questionnaire concerns mainly the protection of children against the criminal exploitation of self-generated sexually explicit images and/or videos and other self-generated sexual contents. Replies by the 42 Parties to the Lanzarote Convention have been published.[67] They will be examined by the Lanzarote Committee in the course of 2018 and 2019 together with comments on the replies submitted by civil society and contributions by children themselves.

Thus, as outlined above, the provisions of the Lanzarote Convention apply to sexual violence in an online environment.

A detailed discussion paper, prepared by the Council of Europe's Global Project on Cybercrime in 2012, showed how the substantive criminal law provisions of the Budapest and Lanzarote Conventions can serve as benchmarks for domestic legislation.[68]

With regard to substantive criminal law, the Budapest and Lanzarote Conventions have a different scope but appear to be complementary. A country implementing the Budapest Convention should thus not limit itself to article 9 Budapest Convention on child pornography but consider also introducing articles 18 to 23 Lanzarote Convention into domestic law in order to cover sexual violence against children.

The Lanzarote Convention does not include specific provisions to secure electronic evidence in domestic and international investigations related to online sexual violence against children. Countries implementing the Lanzarote Convention should thus consider introducing the procedural powers of articles 16 to 21 Budapest Convention into domestic law and becoming Parties to the Budapest Convention to facilitate international cooperation on electronic evidence (articles 23 to 35 Budapest Convention) in relation to online sexual violence against children.[69]

2.4.2 Istanbul Convention on violence against women and domestic violence (CETS 210)[70]

The Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention, CETS 210) defines "violence against women" in article 3:

> as a violation of human rights and a form of discrimination against women and shall mean all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.

The conduct covered by several substantive criminal law provisions may take place, at least partially, in an online environment. Those provisions are thus relevant for the present mapping study:

> Article 33 – Psychological violence
> Parties shall take the necessary legislative or other measures to ensure that the intentional conduct of seriously impairing a person's psychological integrity through coercion or threats is criminalised.

[67] The questionnaire and replies received are available at https://www.coe.int/en/web/children/2nd-monitoring-round
[68] https://rm.coe.int/16802fa3e2
[69] As noted elsewhere, while it is optimal for countries to be Parties to the Lanzarote, Istanbul, and Budapest conventions, non-Parties may of course draw from those conventions to enact domestic legislation.
[70] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/210
GREVIO is the independent expert body responsible for monitoring the implementation of the Istanbul Convention. http://www.coe.int/en/web/istanbul-convention/grevio

> Article 34 – Stalking
> Parties shall take the necessary legislative or other measures to ensure that the intentional conduct of repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for her or his safety, is criminalised.
>
> Article 40 – Sexual harassment
> Parties shall take the necessary legislative or other measures to ensure that any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment, is subject to criminal or other legal sanction.

None of these articles explicitly mentions ICTs, but the Explanatory Report, with regard to article 34, takes into consideration that the threatening behaviour may consist of repeatedly following the victim in the virtual world (chat rooms, social networking sites, instant messaging, etc.). Engaging in unwanted communication entails the pursuit of any active contact with the victim through any available means of communication, including modern communication tools and ICTs.

GREVIO is the independent expert body responsible for monitoring the implementation of the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence.[71] GREVIO underlines the "importance of viewing cyber violence and offline forms of violence against women and girls as an expression of the same phenomenon, namely gender-based violence. Online violence against women and girls should therefore be seen as a continuum of offline violence and as a means to maintain women in an inferior position in the digital sphere and in real life."[72]

In Chapter III (Prevention), article 17 of the Istanbul Convention specifically refers to the participation of the "information and communication technology sector":

> Article 17 – Participation of the private sector and the media
>
> 1. Parties shall encourage the private sector, the information and communication technology sector and the media, with due respect for freedom of expression and their independence, to participate in the elaboration and implementation of policies and to set guidelines and self-regulatory standards to prevent violence against women and to enhance respect for their dignity.
>
> 2. Parties shall develop and promote, in co-operation with private sector actors, skills among children, parents and educators on how to deal with the information and communications environment that provides access to degrading content of a sexual or violent nature which might be harmful.

In 2016, the Council of Europe issued a publication on article 17[73] that identifies four possible actions that governments, the private sector and the media can take together to promote measures to prevent violence against women and domestic violence:

- enhance the training of media professionals on issues related to gender equality and violence against women;
- promote media self-regulation and regulation of discriminatory and violent content;

[71] https://www.coe.int/en/web/istanbul-convention/grevio
[72] GREVIO comments on an earlier draft of the present mapping study.
[73] See 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 https://rm.coe.int/16805970bd (link checked last 19 May 2017). This publication does not necessarily represent an official position of the Council of Europe or of the Parties to the Istanbul Convention.

- create partnerships to increase media coverage of gender equality and violence against women;
- promote co-operation on media literacy.

Article 17 is about prevention and these actions – and the same applies to the detailed "checklist" at the end of the publication – are thus meant to be preventive and do not address criminal justice matters.

The Council of Europe's Gender Equality Strategy (2018-2023) comprises as its first strategic the preventing and combating of stereotypes and sexism, including that which occurs online.[74]

What has been observed with respect to the complementarity of the Budapest and Lanzarote Conventions may apply modus modendi to the Istanbul Convention:

- With regard to substantive criminal law, the Budapest and Istanbul Conventions appear to be complementary. A country implementing the Budapest Convention should thus consider also implementation of articles 33, 34 and 40 Istanbul Convention in order to combat psychological violence, stalking and sexual harassment in an online context.[75]

- Conversely, the Istanbul Convention does not include specific provisions to secure electronic evidence in domestic and international investigations related to online violence against women. Countries implementing the Istanbul Convention should thus consider implementing the procedural powers of articles 16 to 21 Budapest Convention and becoming Parties to the Budapest Convention to facilitate international cooperation on electronic evidence (articles 23 to 35 Budapest Convention) in relation to online violence against women.

2.5 Review of other national and international responses

Governments have adopted a wide range of legal and other responses and the international community has adopted numerous binding and non-binding instruments on the protection of children and on violence against women or family violence (see appendix). Most of these are not specifically aimed at cyberviolence but can be applied off- and online.

The following examples are illustrations of some of the national and international responses on prevention, protection, prosecution and criminalisation.[76]

2.5.1 Prevention

A wide range of initiatives are being undertaken by governments, civil society, private sector and international organisations – frequently in partnership – to prevent cyberviolence, as the following examples illustrate.

Andorra has issued a National Plan of prevention of Bullying and Harassment at School 2016-2019, which identifies four typologies of harassment, namely physical, verbal, social exclusion and cyber harassment, and detailed instruments for prevention.

[74] https://www.coe.int/en/web/genderequality/gender-equality-strategy

[75] Considering that gender-based cyberviolence is a continuum of offline violence a holistic approach is required, covering all provisions of the Istanbul Convention rather than focusing on these three provisions only.

[76] With regard to the "protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies" see also the replies to a questionnaire by Parties to the Lanzarote Convention within the framework of the 2nd round of monitoring by the Lanzarote Committee. https://www.coe.int/en/web/children/2nd-monitoring-round

Austria, with the help of the Association of Internet Service Providers (ISPA), has issued an informative book in German, English and Arabic for children in order to make them aware about the risks on the Internet.

In **France**, the Secrétariat d'État en charge de l'égalité entre les femmes et les hommes has issued for 2017-2019 the *5ème plan de mobilisation et de lutte contre les violences*. This plan aims to pursue three objectives:[77]

- Secure and strengthen proven mechanisms to improve the path of women who are victims of violence and ensure access to their rights;
- Strengthen public action where the need is greatest;
- Root out violence through the fight against sexism, which banalizes the culture of violence and rape.

Part of this plan is devoted to the exposure to harmful content on the Internet, in particular for young women.

In **Germany**, the Government supports some initiatives in this area. For example, in 2016 the 2nd Cybermobbing Congress was 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 the Interior.

In **Italy**, the Ministry of Education has launched a specific campaign to address cyberbullying, creating a permanent observatory for every region of Italy and publishing educational materials (text and multimedia) on a specific website. Part of this plan was the establishment of a national emergency number with a task force composed by experts able to provide the first help in case of cyberbullying. In this campaign an important role was assigned to specific rehabilitation measures, trying to keep the perpetrator and his or her family aware of the consequences of his or her actions. Recently, Italy approved a specific law to combat cyberbullying, and thus further initiatives are expected in the forthcoming months.

Japan has a comprehensive plan called "Basic Plan on Measures against Child Sexual Exploitation"[78] with 88 measures under six pillars, namely:

- Enhancement of public awareness for the eradication of child sexual exploitation, development of social awareness, and the strengthening of collaboration with international society;
- Support for children and families to ensure the sound growth of children without victimization by sexual exploitation;
- Promotion of measures to prevent the occurrence and spread of victimization that focuses on tools used for child sexual exploitation;
- Prompt protection of child victims and the promotion of appropriate support;
- Strengthening of crackdowns based on the situation of victimization and the rehabilitation of offenders;
- Strengthening of the foundation for realizing a society where children will never become victims of sexual exploitation.

[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.

[78] See http://www.npa.go.jp/safetylife/syonen/no_cp/measures/index_e.html (link checked last 11th of May 2018).

In **Mauritius**, the National Computer Board has issued a Guideline on Social Networks[79] and a booklet entitled "Online Responsible Choices for Youngsters"[80] that is an awareness campaign with considerations on combating cyberbullying and cyberviolence, focusing on the idea of respecting the rights of others online, especially human rights.

Mexico has a National Cybersecurity Strategy promoted since 2017 by the Federal Government, and aligned with this strategy, the Federal Police has promoted a National Prevention Campaign called "Cybersecurity Mexico" that has reached directly more than 680,000 citizens and generated more than 48 million interactions in social networks and electronic media. This campaign seeks to raise awareness in Mexican society about the responsible use of new technologies and the Internet to reduce the damage caused by cybercrime. It includes ongoing cybersecurity information days against child sexual exploitation. Additionally, since 2015, National Cybersecurity Weeks have been organized in collaboration with the Organization of American States, with the aim of consolidating awareness efforts in Mexican society.

In **Norway**, several public and private initiatives have been undertaken. This includes the partially publicly-financed service SlettMeg.no ("DeleteMe"). This service was started and formerly run by the Norwegian Data Protection Authority, but is now a separate entity. The main service is a website that has collected information about how to get in touch with various Internet and social media services to remove or de-link unwanted content. SlettMeg.no also offers an answering service for people with questions about how to remove unwanted content. In some cases, SlettMeg.no has also assisted in contacting service providers. In addition, in one recent court case, a senior advisor from SlettMeg.no gave expert witness testimony regarding its experience on the effects and consequences of unwanted private content on the Internet, including sexual content. In addition to public financing, SlettMeg.no also gets support and assistance from a telecom company.

Barnevakten is an NGO focusing on information, focusing on school children and their parents. One of their initiatives, "Bruk Hue" ("Use your head") is a project to fight Internet harassment. This is done in cooperation with other organisations and is supported by several parties, including a telecom company and the Norwegian Media Authority. By visiting schools, this project aims to increase awareness of this issue and to assist children and youth in taking good choices online. Since 2009, this project has visited 1000 schools and talked to 250,000 children and 50,000 parents about digital harassment and good conduct online. According to their own statistics, 7 out of 10 children say, after the school visit, that they now know how to handle digital harassment. 9 out of 10 parents say that, before the school visit, they knew nothing about this problem and/or possible solutions.

The Norwegian Media Authority also runs its own project, Trygg Bruk ("Safe Use"), to assist children and youth to have a safer and better digital life. In cooperation with an NGO, it runs the Norwegian Safer Internet Centre (SIC Norway). This centre has an advisory board that includes people representing the Norwegian police, ICT Norway, the University of Oslo and others.

Singapore puts emphasis on promoting "cyber wellness" within the education system. Cyber Wellness (CW) refers to the positive well-being of Internet users. It involves an understanding of online behaviour and awareness of how to protect oneself in cyberspace. The Ministry of Education uses the CW framework to develop the child's instinct to protect and empower him/her to take responsibility for his/her own well-being in cyberspace. CW Education in Singapore comprises a) CW lessons in the formal curriculum and b) the school-wide programmes (e.g. CW assembly talks, CW activities) to reinforce the importance of CW and its messages. Schools are guided by the CW

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

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

framework to plan and implement CW education which is customised to the student profile and school environment.

The **Council of Europe** has been promoting the protection of children and their empowerment in a digital environment for many years, including through the current "Council of Europe Strategy for the Rights of the Child" [81] which states that children:

> "... have the right to learn, play and communicate online – and to be protected from bullying, hate speech, radicalisation, sexual abuse, and other risks of the "dark net". Guaranteeing the rights of the child in the digital environment is a key challenge all member States of the Council of Europe face, and the Strategy will help them provide children with practical knowledge of how to be online and stay safe."

A range of educational materials and guidelines has been made available.[82]

The Council of Europe has declared 18 November as the "European Day on the Protection of Children against Sexual Exploitation and Sexual Abuse" and focused the 2017 edition on the "protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs)".[83] Several tutorials were made available regarding sextortion, sexting, grooming, "revenge porn" and others.

Another educational campaign, called the "No Hate Speech Movement"[84], has been run by the Council of Europe since 2012. This campaign aims to combat online racism and discrimination by mobilising young people and youth organisations to recognise and act against these human rights violations. The campaign was extended to the end of 2017 as part of the Council of Europe Action Plan on the Fight against Violent Extremism and Radicalisation Leading to Terrorism and pursued the following objectives:

- organise educational activities in and out of schools based on the Bookmarks manual on combating hate speech online through human rights education;
- recognise hate speech as a human rights abuse and incorporate this principle into human rights and citizenship education programmes;
- mobilise and co-ordinate with European and national partners as well as with law-enforcement agencies and national monitoring bodies concerning the response against hate speech;
- develop and disseminate tools and mechanisms for reporting hate speech, especially at national level;
- promote 22 July as the European Day for Victims of Hate Crime;
- place a special focus on hate speech directed at refugees and asylum seekers, sexist hate speech, and anti-Semitism, while taking into account the root causes of violent extremism;
- develop counter-narratives against hate speech;
- create greater regional co-operation to support national campaigns;
- support the implementation of the Council of Europe's relevant instruments, such as the guide, "Human Rights for Internet Users," the general recommendation of the European Commission against Racism and Intolerance on combating hate speech and the Additional Protocol to the Budapest Convention on Cybercrime on xenophobia and racism.

[81] http://www.coe.int/en/web/children/children-s-strategy
[82] http://www.coe.int/en/web/children/the-digital-environment#{"12440617":[4]}
[83] https://www.coe.int/en/web/children/2017-edition
[84] See https://www.nohatespeechmovement.org/ (link checked last 28th of July).

With regard to specifically sexist hate speech, a background note has been prepared by the Council of Europe's Gender Equality Unit.[85]

Article 9 Budapest Convention covers child pornography involving real children who are victims, but also persons appearing to be minors as well as realistic (morphed) images, that is, situations without a real child as a victim. Requiring criminalisation of related acts through article 9.2.b and 9.2.c thus has a protective function and is to prevent a "subculture favouring child abuse".[86]

Article 25 of the European Union Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography is also to "facilitate prevention and mitigate secondary victimisation". It obliges EU member States to promptly remove child abuse materials within their territory and to endeavour to secure removal of materials hosted elsewhere. It furthermore offers the possibility to block access to child pornography. In December 2016, the European Commission published an assessment of the implementation of article 25.[87]

The prevention of sexual abuse and sexual exploitation is also one of the aims of the Lanzarote Convention (see article 1(a) and chapter II).

Chapter III of the Istanbul Convention covers a range of measures to prevent violence against women and family violence, from promoting changes in social behaviour to awareness and education and preventive intervention and treatment programmes.

2.5.2 Protection

Protective measures often focus on the protection of children against sexual exploitation and sexual abuse. For example, Chapter IV of the **Lanzarote Convention** comprises protective measures and assistance to victims, requiring Parties to "establish effective social programmes and set up multidisciplinary structures to provide the necessary support for the victims, their close relatives and for any person who is responsible for their care." These general principles are to be achieved by:

- ensuring that confidentiality obligations of certain professionals called to work in contact with the victim are not an obstacle to their reporting of sexual abuse;
- encouraging and supporting the set-up of information services, such as telephone or Internet helplines, able to guarantee confidentiality and anonymity to the victims;
- providing assistance to the victims, in the short and long term, in their physical and psycho-social recovery.

Hotlines to (a) receive complaints for child abuse and violence against women and leading to investigations or removal of content, or (b) serve as helplines to assist victims, have been available for many years. From the mid-1990s, hotlines began increasingly to address illegal material on the Internet.

Several associations are now in operation in Europe, USA, Canada and other countries that promote good practice, support the development of new hotline initiatives, exchange reports on illegal materials and work together to promote awareness.

The factors that justify the rapid growth of hotlines have been described as follows:[88]

[85] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168059ad42)
[86] See paragraph 102 of the Explanatory Report to the Budapest Convention.
[87] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0872&from=EN
[88] See N. WILLIAMS, *The Contribution of Hotlines to Combating Child Pornography on the Internet*, available at http://www.childnet.com/ufiles/combating-child-pornography.pdf (link last checked 1st June 2017)

- The Internet is the "perfect medium" for paedophiles because:
  - it allows people with the same interest to gather online even if they did not previously know each other;
  - it permits several methods for publishing and exchanging images;
  - it facilitates meticulous organization and storing of images;
  - it permits children to be contacted and enticed into an online or offline relationship.

- The Internet caused also the switch from private exchanges of non-digital images and films to an instant transfer of material in a medium which is easily accessible for everyone.

- The police in different countries were dealing with the fact that much of the material was originating outside their jurisdiction but widely available within it.

- There is pressure on politicians to respond to these threats.

- Internet users are concerned about possible danger to their freedom of expression, thus they are asking for a balanced regulation of the phenomenon and safeguards against unreasonable surveillance.

In this context, hotlines were seen as an appropriate approach because they can be created without changes to legislation, can provide a first answer to public complaints and participate actively in designing procedures to report illegal content.

A leading example of cooperation among national hotlines is **INHOPE** (International Association of Internet Hotlines)[89]. It is a network of associations focused on responding to criminally illegal content and activity, in particular concerning child sexual abuse material, online grooming and online hate including xenophobia.

In particular, the platform for reporting child abuse material presents an interface where it is possible to choose a location and from there to be connected with the local hotline of a specific country.

Some countries, i.e. **Germany** and **Italy**, have more than one association active on the same subject.

In the **UK** a hotline has been created and is managed by the Child Exploitation and Online Protection Centre (CEOP) of the National Crime Agency[90] that permits a person in a few easy steps to report possible situations of danger, such as requests for nude images, online threats, requests for meeting face-to-face or via webcam, cyberbullying, etc. A Child Protection Advisor at CEOP may offer assistance to keep the possible victim safe.

In the **Netherlands** the local branch of the INHOPE hotline (Expertise centrum online misbruik kinderen; Centre for expertise on online child sexual abuse[91]) operates an actual hotline as well as a website with information and associated chat or other contact methods called "help wanted." This website is mainly directed against sextortion and other unwanted publications of often self-generated images.

[89] http://www.inhope.org/gns/home.aspx
[90] See the CEOP (Child Exploitation and Online Protection command) at https://ceop.police.uk/safety-centre/ (link checked last 1st June 2017).
[91] https://www.eokm.nl/

In **Israel**, the Ministry of Public Security, together with the Israeli Police, has recently founded a unit dedicated to tackle offences committed against minors online. The new unit, named "the 105 unit", will operate in four different levels: First, the unit includes a national call center regarding minor-related offences; Second, the unit includes a special investigation unit which will focus on revealing and investigating online offences against minors; Third, the unit will take part in activities in the fields of education, welfare and the prevention of suicide among minors; Fourth, the unit will be active on the matter of content removal, when the content is harmful to minors (such as "revenge porn" or the violation of non-publication warrants related to minors).

Some national plans provide also actions or instruments to protect the victims. In **France**, for example, one of the objectives[92] of the French plan to fight violence foresees the protection of the victims of cybersexism through different actions:

- Facilitate the reporting of acts of cybersexism;
- Enforce the new legislation and its aggravated sanctions for sexual cyberviolence;
- Distribute a guide on sexual cyberviolence and possible remedies.

Mexico has established the National Center for Attention to Cybercrimes against Minors (CENADEM) within the Scientific Division of the Federal Police.

The CENADEM is the unit in charge of collaborating with the executive, federal and judiciary authorities, social actors, academic institutions and civil society, through follow up to citizen's reports, ministerial and judicial orders, monitoring of the public internet social networking, and cooperation with national and international organizations in order to prevent, investigate and fight crime or antisocial behaviour that are committed in electronic, cybernetic or technological media, related to human trafficking and child sexual exploitation. This unit receives citizen's complaints through a direct line of the Federal Police, the telephone number 088 works throughout the whole country, to support victims of cybercrime.

2.5.3 Prosecution

The cases provided by Parties and Observers to the T-CY (see appendix) are examples of successful prosecutions of different types of cyberviolence in Andorra, Austria, Chile, France, Israel, Japan, Latvia, Mauritius, Netherlands, Philippines, Slovakia, Slovenia and USA.

Age is a decisive criterion when it comes to the prosecution of cyberviolence. Many States have set up special units to investigate and prosecute the sexual exploitation and abuse of children online.

This is less the case if victims of cyberviolence are adults.

An exception may be "hate crime". In the **United Kingdom**, for example, the Crown Prosecution Service published statements in August 2017 "on how it will prosecute hate crime and support victims in England and Wales". Hate crime is defined as follows:[93]

> The police and the CPS have agreed the following definition for identifying and flagging hate crimes:
> "Any criminal offence which is perceived by the victim or any other person, to be motivated by hostility or prejudice, based on a person's disability or perceived disability; race or perceived race; or religion or perceived religion; or sexual orientation or perceived sexual orientation or a person who is transgender or perceived to be transgender."

[92] See Objectif 24 of the 5ème plan de mobilisation et de lutte contre les violences.
[93] https://www.cps.gov.uk/hate-crime

> There is no legal definition of hostility so we use the everyday understanding of the word which includes ill-will, spite, contempt, prejudice, unfriendliness, antagonism, resentment and dislike.

In 2015/2016, the CPS had prosecuted 15,442 hate crimes, 84% of which were "racially and religiously aggravated crime cases." An increase of 41% in "disability hate crime" was noted compared to the previous year.[94]

The conviction rate is more than 80%:

> More than four in five prosecuted hate crimes result in a conviction, which is good news for victims. Over 73 per cent are guilty pleas - this means that more defendants are pleading guilty due to the strength of the evidence and prosecution case, so victims do not have to go through the process of a trial.

The CPS has published "Prosecution Guidance" on "racist and religious hate crime," [95] "homophobic, biphobic and transphobic hate crime" [96] and "disability hate crime."[97]

2.5.4 Criminalisation of cyberviolence

While most States have legislation criminalising conduct related to online sexual exploitation and abuse of children,[98] the criminalisation of other forms of cyberviolence such as cyberbullying, harassment, sextortion and others is a more recent development. Some laws include liability of service providers. Most States seem to apply regular criminal law and other provisions. For example:[99]

- **Austria** criminalises in §107c of the Penal Code the "Persistent harassment involving telecommunication or computer systems":
  "(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."

- **Chile** adopted in 2011 a "School violence law" amending the General Education Act to prevent psychological and physical violence in school, including bullying. The law does not impose criminal sanctions.

- In 2016, **France** adopted the 'Digital Republic Law,' which entails a harsher sanctioning of those found guilty of revenge porn. Under the new legislation, perpetrators face a two-year prison sentence or a € 60 000 fine.

---

94 http://www.cps.gov.uk/news/latest_news/more_hate_crimes_prosecuted_by_the_crown_prosecution_service_than_ever_before/

95 http://www.cps.gov.uk/legal/p_to_r/racist_and_religious_crime/

96 http://www.cps.gov.uk/legal/h_to_k/homophobic_and_transphobic_hate_crime/

97 http://www.cps.gov.uk/legal/d_to_g/disability_hate_crime/

98 For examples of criminalisation see 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.

99 These are examples for illustration. See appendix for more information on legislation in Parties and Observer States.

- **Germany** – like many other States – makes use of criminal law provisions that are not specific to the online environment, such as section 238 of the German Criminal Code (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*) as well as section 33 of the Law concerning copyright related to works of visual arts and photography (*Kunsturhebergesetz*). Section 238 (Stalking) expressly 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).
  The Act to Improve Enforcement of the Law in Social Networks (in force since June 2017) is to enforce compliance obligations for social networks, but is not extending the scope of criminalization. In particular, social networks with more than 2 million registered users are required to provide an effective complaints management, and to remove or block 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 for example with regard to 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.

- **Israel** also applies provisions of the Criminal Code and other laws, such as the Protection of Privacy Act (1982) or the Prevention of Sexual Harassment Act (1998) for conduct online. For example, article 3(a) of 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 if 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 "cyber-bullying".

- **Italy** in May 2017 adopted law no. 71/2017, entitled "Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying". Article 1 of the law defines cyberbullying as "whatever form of psychological pressure, aggression, harassment, blackmail, injury, insult, denigration, defamation, identity theft, alteration, illicit acquisition, manipulation, unlawful 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.

- **Japan** has adopted the Anti-stalking Act which covers "Making silent calls, or calling, transmitting using a fax machine or sending text messages through any text messaging service persistently despite his/her rejections" …. "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." Other provisions of the Penal Code on intimidation (article

222(19)), compulsion (223(1)), defamation (230(1) or insults (231) may also be applied.

- **Liechtenstein** applies provisions of its Criminal Code, such as § 105 – Coercion, § 106 - Aggravated coercion, § 107 - Dangerous threat, § 107a - Persistent stalking, § 111 – Defamation, § 112 - False accusation, or § 115 – Insult, but also offences against computers and data.

- **Slovakia** has no specific provisions on "cyberviolence" but applies a wide range of provisions of the Criminal Code such as 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 Crimes against Humanity (Section 422d of CC), Defamation of Nation, Race and Conviction (Section 423 of CC), or Incitement to National, Racial and Ethnic Hatred (Section 424 of CC).

- In the **UK**, in April 2015 it became a criminal offence with a maximum of two years imprisonment to share private sexual photographs or videos without the subject's consent with the intent of causing distress to those targeted. In September 2016 it was announced that more than 200 people had been prosecuted since the law came into effect.

- The **USA** criminalises "cyberstalking" in 18 US 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 …"
  The USA also has a specific provision on "extortion involving computers" (18 US Code Section 1030(a)(7)) which includes threats to cause damage to a computer or threats to obtain information from a protected computer.

With regard to the criminalisation of cyberviolence the following observations can be made:

- Domestic law alone may not always be enough, particularly when offenders commit crimes in multiple countries, attempting to hide their identity and evade capture. In general, the Budapest Convention is likely to be useful in the investigation of many forms of cyberviolence, either because a Budapest Convention provision criminalizes an act or because the procedural provisions under the Convention are useful for the collection of evidence or international cooperation.

- With regard to sentencing, the Cyberviolence Group suspects that countries do not always punish cyberviolence to a degree that is appropriate to the harm done. It found limited data to support this thesis as well as the thesis that cyberviolence is not punished to a degree consistent with physical-world harms, even if the injury to the victim is extreme.[100] Article 13 of the Budapest Convention requires countries to enact effective, proportionate, and dissuasive sanctions, including deprivation of liberty and monetary sanctions as appropriate. This standard should also be applied to prosecutions of cyberviolence where it constitutes a criminal offence.

- The European Court of Human Rights held in K.U. v. Finland,[101] that States have a positive obligation to protect citizens against crime, including invasions of private life. Law enforcement therefore has an obligation to conduct investigations and prosecutions of acts of cyberviolence. States must take cyberviolence seriously and see to it that laws are amended, investigative skills improved, etc.

- Cyberviolence targets many people based on their characteristics or membership in certain groups. Physical-world legislation in different countries protects different social groups and it would not be possible to list all the bases on which people are targeted or specially protected. However, some familiar bases would be: age, citizenship, colour, ethnicity, language, marital status, national origin, physical challenges, race, religion, sex, sexual orientation, and social status (military veteran, police officer, refugee, and others).[102] Victims may of course be targeted for more than one reason.

- Much of this report is entirely relevant, and readily extensible, to victims other than women and children. The attacks may be similar and legal protections equally available or inadequate.

- Because cyberviolence may be related to or lead to physical consequences, including physical attacks, countries should ensure that their online and offline laws are consonant: electronic threats may be no less terrifying than threats on paper. In addition, laws must be written in technologically-neutral terms while being concise and differentiated at the same time. As electronic crime develops, flexibly-drafted laws will best be able to address it.

[100] WITTES, Benjamin, et. al., "Closing the sextortion sentencing gap: a legislative proposal," Brookings Institution, May 2016, https://www.brookings.edu/research/closing-the-sextortion-sentencing-gap-a-legislative-proposal/ (link last checked on 11 November 2017).
[101] See *K.U. v. Finland* 02.12.2008 (European Court of Human Rights, no. 2872/02).
[102] Cyberviolence also affects people who are not themselves the targets – parents of targeted children, for example.

3 Cyberviolence against women and children: the role of the Budapest Convention

3.1 Substantive law

Articles 2 through 11 constitute the Budapest Convention's substantive criminalisation section. Three articles could be utilized in connection with cyberviolence.[103] Other substantive articles criminalise acts that could be involved in cyberviolence, but the connection is less direct. Such acts could facilitate violence and could be prosecuted, but they would not criminalise the violence itself.

3.1.1 Articles with a more-direct connection to cyberviolence

- Article 4 – Data interference in a critical system may cause death or physical or psychological injury.
- Article 5 – System interference in a critical system may cause death or physical or psychological injury.
- Article 9 – Child pornography. Article 9 (1) (a) criminalises producing child pornography for electronic distribution. Production of child pornography may cause death and necessarily entails physical and/or psychological violence.

Other sub-provisions of article 9 cover the distribution of child exploitation images; that distribution may itself inflict psychological violence. Such provisions include 9 (1) (b), offering or making child pornography available; 9 (1) (c), distributing or transmitting it; and 9 (1) (d), procuring child pornography for another person (for example, a child forced to view another child's exploitation).[104]

3.1.2 Articles with a facilitating connection to cyberviolence

This section provides examples, not an exhaustive list, of the ways in which acts that can facilitate violence are covered by other articles of the Budapest Convention. Law enforcement experience, media reports, or imagination would readily provide other examples.

- Article 2 – illegal access to a victim's system is common in cyberthreats, cyberstalking, sextortion, and other forms of privacy violations amounting to cyberviolence. A third party's system may be accessed illegally to be used as a platform for messages or attacks or for the theft of intimate data.
- Article 3 – incoming or outgoing traffic may be illegally intercepted to hinder communication with law enforcement or to show a victim that the attacker is aware of everything the victim does. Traffic may also be intercepted to commit privacy violations amounting to cyberviolence.
- Articles 4 and 5 have a facilitating as well as a direct connection to violence.

[103] These crimes could target any class of person, not just women and children. (Article 9 (2) (b) indicates how Article 9 could cover men who appear to be children.)

[104] It is important to note that the Lanzarote Convention (Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote, 27 October 2007)) is the primary source of law for its Parties on this subject and may provide guidance for non-Parties. Other international instruments that address child exploitation are also important.

- Article 4 – data interference could alter a person's social media postings to attract hostility.

- Article 5 – system interference. An attacker who sends death threats may take sufficient control of a computer system that a victim may be unable to preserve threatening messages.

- Article 6 – misuse of devices. A criminal may harvest passwords from a target system – a school, an organisation, etc. – to use its internal system to transmit threats.

- Article 7 – computer-related forgery may be used to fake authorisation to enter a building.

- Article 11 criminalises attempting, aiding, and abetting some or all (depending on the circumstances) of the crimes in articles 2 through 10. It could be used to address cyberviolence in conjunction with articles 4, 5, and 9. However, to charge *attempt* to commit one of the other *facilitating* crimes would be a very indirect method of addressing violence.[105]

3.2 Procedural law

Article 14 provides that countries must apply the Budapest Convention's procedural law provisions to the substantive offences in the Convention, to other criminal offences committed by means of a computer system, and to the collection of evidence in electronic form of any criminal offence.[106]

The procedural tools thus are available to pursue cyberviolence in any form. Those tools include:

- expedited preservation (article 16);
- preservation and partial disclosure (article 17);
- production orders (article 18);
- search and seizure of stored data (article 19);
- real-time collection of traffic data (article 20);
- interception of content data (article 21).

3.3 International cooperation

Article 23 requires Parties to cooperate to the greatest extent possible under any relevant instrument or law "for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."

The international cooperation provisions of the Budapest Convention include:

- extradition (article 24);
- general cooperation principles (article 25);
- spontaneous information (article 26);
- mutual assistance in the absence of international agreements (other than Budapest Convention) (article 27);
- confidentiality and use limitations (article 28);
- expedited preservation (article 29);
- expedited disclosure of traffic data (article 30);

[105] The same would be true for charging aiding or abetting.
[106] Limited reservations are permitted. See Article 14.

- mutual assistance in accessing of stored data (article 31);
- transborder access to stored data (article 32);
- mutual assistance in the real-time collection of traffic data (article 33);
- mutual assistance in the interception of content data (article 34).

Some provisions permit the application of the doctrine of dual criminality or they incorporate domestic law by reference. Whether dual criminality and domestic law are applied rigidly or flexibly is particularly important in cyberviolence cases, because a) the cases frequently have a transnational element, and b) as of this writing, countries have not systematically criminalised novel and varied forms of cyberviolence.

3.3.1 Preservation

Preservation is the most basic, least-intrusive tool in electronic investigations. Thus, article 29 does not permit Parties to refuse preservation based on dual criminality except in limited circumstances. If a Party normally requires dual criminality to search, secure or disclose stored data, it may also refuse to *preserve* data if it believes that the requesting Party will not be able to satisfy dual criminality when requesting *disclosure* and if the crime involved is not covered in articles 2 through 11. However, this only applies to Parties that have deposited a reservation regarding article 29.4.

As discussed, cyberviolence is only partially covered by articles 2 through 11. For preservation to function in these cases, either a) Parties should apply dual criminality flexibly, or b) requesting Parties must seek preservation based on one of the facilitating crimes in articles 2-7 and 11. For example, a Party might seek preservation in a cyberthreats case based on article 2, illegal access to a victim's computer.

3.3.2 General cooperation principles

Article 25 initially repeats statement of article 23 that Parties shall afford each other the widest possible mutual assistance, including for the collection of evidence in electronic form of a criminal offence. Article 25 later declares that, when a Party evaluates dual criminality, it must ask if the conduct underlying the offence for which assistance is sought is a criminal offence under its own laws. The Party is not permitted to focus on whether the offence is within the same category of offence, or called by the same name, as in domestic law. The article emphasizes flexibility so that new crimes can be pursued.

3.3.3 Mutual assistance in accessing of stored data

Article 31 incorporates by reference certain "international instruments, arrangements and laws" as well as "other relevant provisions of this chapter." The incorporation by reference of those instruments, arrangements, laws, and other provisions may mean that dual criminality or domestic law may affect cooperation in cyberviolence cases.

3.3.4 Mutual assistance in the real-time collection of traffic data and mutual assistance in the interception of content data

Articles 33 and 34 incorporate domestic law in their terms. Under article 33, Parties must collect traffic data for each other in real time "at least with respect to criminal offences for which [such collection] would be available in a similar domestic case." Article 34 requires Parties to collect or record content data "to the extent permitted under … domestic laws."

A country's current domestic law may not cover cyberviolence offences per se. If that is the case, the requested country may be able to extract elements from the requesting country's submission to be able to cooperate. For example, a country might rely on the fact that threats were sent

without regard to the fact that they were sent electronically. But if domestic law does not cover an offence per se and if usable elements cannot be extracted from an MLA request, international cooperation to obtain traffic or content data may be blocked.

3.4 The question of a Guidance Note

Three of the substantive provisions of the Budapest Convention have a direct connection to cyberviolence. Other provisions cover (chargeable) conduct that may facilitate such violence. The procedural tools would apply in either case. The Convention's international cooperation tools would also apply to any case, but several of the important tools might be impeded by the doctrine of dual criminality or by domestic law.

A T-CY Guidance Note could explain the above. However, it may only offer a partial solution. It would thus seem advisable to consider providing guidance on how the Budapest Convention and its Protocol on Xenophobia and Racism could be applied in conjunction with the Istanbul and Lanzarote Convention, rather than preparing a Guidance Note on the provisions of the Budapest Convention as such.

4 Findings and recommendations

4.1 Findings (gaps and issues)

4.1.1 On the concept of cyberviolence

Cyberviolence may be defined provisionally as:

> the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities.

This includes cyberharassment (including cyberbullying), forms of violation of privacy, the online sexual exploitation and sexual abuse of children. Some forms of cybercrime as well as direct threats of or actual violence may also constitute cyberviolence.

Forms of cyberviolence may represent violations of human rights and forms of discrimination.

The concept of cyberviolence as used in this study remains elusive and difficult to delimit. More research is needed to arrive at a mature concept of cyberviolence.

4.1.2 Cyberviolence: Scope, impact and issues

Cyberviolence is violence against individuals with often devastating consequences for individuals. While the consequences of cyberviolence may not in every case be equated to the consequences of physical violence, cyberviolence should be of primary concern to societies.

Many forms of violence that are now associated with cyberviolence, in their physical world manifestation, have always been issues that societies had to deal with, among other things, through criminal law (coercion, threats, false accusation, insult, defamation, harassment, extortion, violation of privacy, rape, etc.).

Physical world solutions to violence may therefore also be applied to address acts of violence if computers are involved.

However:

- While physical world violence is normally limited by the need for face-to-face interaction or the limits of more traditional means of communication, there are few barriers to cyberviolence committed via computer systems. In particular, social media and the vastly-increased collection, public availability, and searchability of information have facilitated a proliferation of cyberviolence. In the physical world it would be impossible to recruit hundreds of men to go to an ex-girlfriend's house to demand sex. It is quite possible to arrange this via the Net.

- Cyberviolence is not simply an extension of physical world violence. The nature and impact of violence seems to have changed if committed by means of computer systems. Specific solutions are therefore required. Cyberviolence may comprise new forms of violence that do not have an equivalent in the physical world or that require more consistent criminalisation in different States to permit international cooperation.

There may be no physical-world crime that repeats or persists after its commission without any action by the criminal, yet this is the case with many forms of cyberviolence. Once material has been posted, copied, re-distributed, etc., the victim's sufferings continue, though the criminal does not need to take any action. This aspect of cyberviolence appears often not to be reflected in sentencing of offenders, while the harmful impact of cyberviolence on victims may essentially be long lasting. They are re-victimised every time a new professional colleague, a romantic partner, prospective in-laws, or someone else researches them online.

4.1.3 National and international responses to cyberviolence

Governments, civil society, private sector and international organisations increasingly adopt policies and measures to address cyberviolence. The primary focus is on prevention and education targeting children and young adults.

Protective measures often focus on the protection of children against sexual exploitation and sexual abuse. Hotlines play an important role in this respect.

Specialised units for the investigation and prosecution of the online sexual abuse of children have been created in a number of States.

However, this seems to be less the case with regard to other forms of cyberviolence.

Many States have criminalized forms of coercion, threats, (sexual) harassment, privacy violations, insults, extortion and other forms of violence, including xenophobia, racism and other forms of hate speech that can also be applied when computer systems are involved. Some forms of cyberviolence may be charged using these and other physical-world laws (solicitation to commit a crime, for example).

Apart from criminalisation of acts related to child sexual exploitation and sexual abuse, specific legal provisions regarding other forms of cyberviolence are less common. Some States indicate that they have criminalized cyberstalking and cyberbullying.

The criminal law response to specific forms of cyberviolence is thus limited for different reasons, including that criminal law responses are not always considered appropriate and other solutions are preferred.

Several issues have been noted:

- Victims of cyberviolence frequently may not know what to do to get help.
- Law enforcement authorities are often not able to assist victims and cyberviolence may not be considered a law enforcement priority or may not be considered sufficiently serious ("we don't do Facebook complaints").
- While solutions to online violence, in particular sexual abuse, against children are available, there are gaps when it comes to responses to online violence against adults.
- Social media providers can play a role in the prevention and control of cyberviolence and in the protection of victims. This role is often considered insufficient.
- The prevention and control of cyberviolence may run counter to the freedom of expression and other rights (e.g. free speech versus hate speech). Where they do not actually conflict, their relationship must still be carefully considered.

4.1.4 Types of cyberviolence addressed or not addressed in international agreements

- The **online sexual exploitation and sexual abuse of children** is covered by the Lanzarote Convention (CETS 201) which also applies if committed by means of computer systems (ICT). However, as this treaty is missing specific procedural powers and means of international cooperation for computer-related investigations and securing electronic evidence, its Parties should be made aware of the tools and means offered by the Budapest Convention and encouraged to use them to effectively address the cyberdimension of sexual exploitation and sexual abuse of children. To this end, Parties to the Lanzarote Convention not having yet ratified the Budapest Convention should do so.
- **Cybercrime**, that is, offences against the confidentiality, integrity and avaibility of computer systems and certain offences by means of computers, may result in physical, sexual, psychological or economic harm or suffering of individuals, and is addressed by the Budapest Convention on Cybercrime in terms of substantive criminal law, backed up by procedural powers and means of international cooperation to investigate and prosecute crimes that may be forms of cyberviolence in some cases. However, sanctions and measures may not always be commensurate in practice to the impact on individuals. Cybercrime may also facilitate other types of cyberviolence.
- **Hate crime** is partly covered by the Additional Protocol to the Budapest Convention on Xenophobia and Racism, and thus addresses cyberviolence motivated by certain biases, but not if motivated by other perceived characteristics such as gender, sexual orientation or disability. The work of the Council of Europe and other organisations on discrimination and intolerance is also relevant. Key issues are the role of service providers and the question of hate speech versus free speech.
- **Direct threats of and physical violence** cover a broad range of conduct that is covered in the domestic law of most States and should also apply if committed by means of computers. Again, the mechanisms in the Budapest Convention may be used for domestic and international investigations. Such direct threats or violence may yield a commensurate criminal justice response.
- **Violations of privacy** involve a range of conduct that may be partly addressed by the Budapest Convention and other treaties (e.g. article 34 of the Istanbul Convention -

Stalking). It is not always evident that such conduct results in a sufficient criminal justice response and that victims will receive the assistance needed.[107] More guidance may help States apply existing provisions effectively and adequately to address this type of cyberviolence. More research would be needed as to whether application of existing provisions is sufficient.

- **Cyberharassment** is the broadest category of cyberviolence and includes, among others, cyberbullying. The Istanbul Convention addresses "psychological violence" in article 33 and "sexual harassment" in article 40, and these concepts could also be applied in connection with cyberviolence.[108] The same may be true for provisions on violence and discrimination against women in international treaties, resolutions and declarations. And many provisions covering forms of violence in domestic law would also apply to cyberviolence. However, while these solutions may provide inspiration, they do not seem to address the specificities of cyberharassment in a satisfactory manner.

4.1.5 Role of the Budapest Convention

The Budapest Convention through a number of substantive criminal law provisions addresses directly some types of cyberviolence. Other provisions address acts facilitating cyberviolence.

The procedural powers and the provisions on international cooperation of the Convention on Cybercrime will help investigate cyberviolence and secure electronic evidence.

The Budapest Convention and treaties such as the Istanbul and Lanzarote Conventions complement each other.

It would seem that more could be done to emphasise such complementarity and to promote synergies between these three instruments.

4.2 Recommendations

Efforts – including joint measures – by a broad range of stakeholders are required to address the multi-facetted problem of cyberviolence.

At the level of the Council of Europe and Cybercrime Convention Committee:

Rec1 The Council of Europe (T-CY Secretariat and C-PROC) should consider making available online information on cyberviolence included in the present study on existing policies, strategies, preventive, protective and criminal justice measures taken by public sector, civil society and private sector organisations, and creating an online portal to receive, document and make available new developments and information on such policies, strategies, preventive, protective and criminal justice measures taken by public sector, civil society and private sector organisations.

Rec 2 Given the difference in scope but given also the complementarity between the Budapest Convention and its Protocol, and the Lanzarote and Istanbul Conventions, Parties[109] – within their respective treaty obligations – and the Secretariat may consider promoting synergies between these instruments in practice, including by:

[107] A criminal justice response may not always be required.
[108] It may be useful to study how Parties to the Istanbul Convention have implemented these provisions.
[109] Bearing in mind that not all Parties to the Budapest Convention are Parties to the Istanbul and Lanzarote Conventions.

- raising awareness among Parties of the provisions of these treaties;
- drawing on these treaties in capacity building activities and when providing advice to countries;
- encouraging Parties to the Lanzarote and Istanbul Conventions to introduce the procedural powers of articles 16 to 21 Budapest Convention into domestic law and to consider becoming Parties to the Budapest Convention to facilitate international cooperation on electronic evidence (articles 23 to 35 Budapest Convention) in relation to online sexual violence against children and violence against women and family violence;
- encouraging Parties to the Budapest Convention to draw on articles 33, 34 and 40 Istanbul Convention to address psychological violence, stalking and sexual harassment in an online context and on the Lanzarote Convention – in particular articles 18 to 23 – to address the sexual exploitation and the sexual abuse of children online, and to consider becoming Parties to these treaties.

Rec 3 Parties to the Budapest Convention should consider better training and awareness raising for criminal justice authorities regarding cyberviolence, including its investigation, prosecution and sanctioning, where it constitutes a criminal offence. The Council of Europe – through its C-PROC – and other organisations should support such capacity building activities. T-CY members may wish to share the present study among relevant institutions within their countries.

Rec 4 Measures to prevent, protect against and – in cases where it constitutes a criminal offence – prosecute cyberviolence should be conceived as contributing to the implementation of the UN Agenda 2030 for Sustainable Development, [110] in particular, Sustainable Development Goal 16 The present study may thus be shared with relevant bodies of the United Nations.

Rec 5 Parties to the Budapest Convention should ensure greater gender balance in institutions dealing with cybercrime.

4.3 Follow up

The T-CY should consider follow up given to these recommendations within 24 months of their adoption.

[110] http://www.un.org/sustainabledevelopment/peace-justice/
Goal 16: "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels" including:
- significant reduction of all forms of violence and related death rates everywhere;
- end of abuse, exploitation, trafficking and all forms of violence against and torture of children;
- rule of law at the national and international levels and equal access to justice for all;
- effective, accountable and transparent institutions at all levels;
- responsive, inclusive, participatory and representative decision-making at all levels;
- strengthened relevant national institutions, including through international cooperation, for building capacity at all levels to prevent violence and combat terrorism and crime;
- non-discriminatory laws and policies for sustainable development.

5 Appendix

5.1 References/sources/bibliography

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 Websites

http://cookie.sk/
www.detinawebe.sk
https://goo.gl/ctBT63 (online questionnaire)
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 (to download for free)

5.3 Links to references provided by Parties and Observers

5.3.1 Austria

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 Italy

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

5.3.4 Mauritius

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 Norway

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

5.4 Relevant international instruments

5.4.1 Binding instruments

5.4.1.1 Council of Europe legally binding instruments

Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocol No. 11) (Roma, 4 November 1950) https://rm.coe.int/1680063765

Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul, 11 May 2011) https://rm.coe.int/168008482e

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote, 27 October 2007)
https://www.coe.int/t/dg3/children/1in5/Source/Lanzarote%20Convention_EN.pdf

Council of Europe Convention on Action against Trafficking in Human Beings (Warsaw, 16 May 2005) https://rm.coe.int/168008371d

European Social Charter (revised) (Strasbourg, 3 May 1996) https://rm.coe.int/168007cf93

European Convention on the Compensation of Victims of Violent Crimes (Strasbourg 24 November 1983) https://rm.coe.int/1680079751

Convention on Contact concerning Children (Strasbourg, 15 May 2003)
https://rm.coe.int/168008370f

Convention on Cybercrime (Budapest, 23 November 2001)
https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

5.4.1.2 United Nations legal instruments

International Covenant on Civil and Political Rights (ICCPR) (New York, 16 December 1966) http://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

International Covenant on Economic, Social and Cultural Rights (ICESCR) (New York, 16 December 1966) http://www.ohchr.org/Documents/ProfessionalInterest/cescr.pdf

Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) (New York, 18 December 1979) http://www.un.org/womenwatch/daw/cedaw/text/econvention.htm

Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women (OP-CEDAW) (New York, 6 October 1999)
https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/774/73/PDF/N9977473.pdf?OpenElement

Declaration on the Elimination of Violence against Women (*proclaimed by General Assembly resolution 48/104 of 20 December 1993,* New York)
http://www.un.org/documents/ga/res/48/a48r104.htm

Convention on the Rights of the Child (CRC) (*adopted and opened for signature, ratification and accession by the General Assembly resolution A/44/25 of 20 November 1989, New York)*
http://www.ohchr.org/Documents/ProfessionalInterest/crc.pdf

Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OP- CRC-SC) (*adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000,* New York*)* http://www.ohchr.org/Documents/ProfessionalInterest/crc-sale.pdf

Optional Protocol to the Convention on the Rights of the Child on a communications procedure (OP-CRC-IC) (New York, 14 April 2014)

http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPICCRC.aspx

General Recommendation No. 19 on violence against women (1992)
http://www.un.org/womenwatch/daw/cedaw/recommendations/recomm.htm#recom19

5.4.1.3 EU legal instruments

Council Directive 97/80/EC on the burden of proof in cases of discrimination based on sex *(adopted on 15 December 1997)*
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997L0080&from=GA

Council Directive 2002/73/EC on the implementation of the principle of equal treatment for men and women as regards access to employment, vocational training and promotion, and working conditions (*adopted by the European Parliament and Council on 23 September 2002)* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0073&from=EN

Council Directive 2004/113/EC on the implementing the principle of equal treatment between men and women in the access to and supply of goods and services *(adopted on 13 December 2004)* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0113&from=EN

Council Framework Decision on the standing of victims in criminal proceedings *(adopted by 15 March 2001)* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001F0220&from=GA

Council Recommendation on the prevention of injury and the promotion of safety *(adopted on 31 May 2007)* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007H0718(01)&from=EN

5.4.1.4 Legal instruments adopted in the framework of other international regional organizations (OAS, OAU)

Inter-American Convention on the prevention, punishment and eradication of violence against women (Belém do Pará, 9 June 1994) http://www.oas.org/juridico/english/treaties/a-61.html

Protocol to the African Charter on Human and Peoples´ Rights on the Rights of Women in Africa (Maputo, 11 July 2003)
http://www.achpr.org/files/instruments/women-protocol/achpr_instr_proto_women_eng.pdf

5.4.2 Soft law/non-binding instruments

5.4.2.1 Council of Europe legally non-binding instruments

Recommendation Rec (2006)8 on assistance to crime victims *(adopted by the Committee of Ministers on 14 June 2006 at the 967th meeting of the Ministers´ Deputies)* https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805afa5c

Recommendation Rec (2005)5 on the rights of children living in the residential institutions *(adopted by the Committee of Ministers on 16 March 2005 at the 919th meeting of the Ministers´ Deputies)* https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805daac2

Recommendation Rec (2002)5 on the protection of women against violence *(adopted by the Committee of Ministers on 30 April 2002 at the 794th meeting of the Ministers´ Deputies)* https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e2612

Recommendation No. R (99)19 concerning mediation in penal matters *(adopted by the Committee of Ministers on 30 April 2002 at the 490th meeting of the Ministers´ Deputies)* https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=090000168062e02b

Recommendation No. R (93)2 on the medico-social aspects of child abuse *(adopted by the Committee of Ministers on 22 March 2002 at the 794th meeting of the Ministers´ Deputies)* https://rm.coe.int/16804eebb5

Recommendation No. R(91) 9 on emergency measures concerning violence within the family *(adopted by the Committee of Ministers on 9 September 1991 at the 461st meeting of the Ministers´ Deputies)* https://rm.coe.int/16804bfa85

Recommendation No. R (85) 11 on the position of the victim in the framework of criminal law and procedure *(adopted by the Committee of Ministers on 28 June 1985 at the 387th meeting of the Ministers´ Deputies)* https://rm.coe.int/16804dccae

Recommendation No. R (85) 4 on violence in the family *(adopted by the Committee of Ministers on 26 March 1985 at the 382nd meeting of the Ministers´ Deputies)* https://rm.coe.int/16804f120d

5.4.2.2 Parliamentary Assembly of the Council of Europe (PACE) legally non-binding instruments (resolutions and recommendations)

Resolution 1654 (2009) on Femicides *(adopted by the PACE on 30 January 2009)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzcxNiZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NzE2

Recommendation 1861 (2009) on Femicides *(adopted by the PACE on 30 January 2009)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzcxNyZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NzE3

Resolution 1635 (2008) on Combating violence against women: towards a Council of Europe Convention *(adopted the PACE on 3 October 2009)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzY4MiZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3Njgy

Recommendation 1847 (2008) on Combating violence against women: towards a Council of Europe Convention *(adopted the PACE on 3 October 2009)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzY4MyZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3Njgz

Resolution 1582 (2007) "Parliaments united in combating domestic violence against women": mid-term assessment of the campaigns *(adopted by the PACE on 5 October 2007)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzU5NCZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NTk0

Recommendation 1817 (2007) on Parliaments united in combating domestic violence against women: mid-term assessment of the campaign *(adopted by the PACE on 5 October 2007)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzU5NiZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NTk2

Recommendation 1777 (2007) on sexual assaults linked to "date-rape drugs" *(adopted by the PACE on 22 January 2007)*

http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzQ5OCZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NDk4

Resolution 1512 (2006) on Parliaments united in combating domestic violence against women *(adopted by the PACE on 28 June 2006)*
http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzQ2NCZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3NDY0

Recommendation 1723 (2005) on forced marriages and child marriages *(adopted by the PACE on 5 October 2005)*
http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzM3OSZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3Mzc5

Resolution 1327 (2003) on so-called "honour crimes" *(adopted by the PACE 4 April 2003)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNzEwNiZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE3MTA2

Resolution 1247 (2001) on female genital mutilation *(adopted by the Standing Committee, acting on behalf of the PACE on 22 May 2001)* http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNjkxNCZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTE2OTE0

Recommendation 1450(2000) on violence against women in Europe *(adopted by the PACE on 3 April 2000)*
http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbnQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0xNjc4MyZsYW5nPUVO&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[111] 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.

[111] 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*[112] issued in April 2017 the *Guide d'information et de lutte contre les cyberviolences à caractère sexiste*[113] 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

[112] 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).
[113] 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*)[114] 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*)[115] 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.

[114] Available online (only in German language): http://www.gesetze-im-internet.de/gewschg/index.html
[115] 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.[116]
   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.

[116] 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[117].

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

[117] 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[118]. In the general framework of this policy, the National Computer Board issued a Guideline on Social Network[119] and a booklet entitled "Online Responsible Choice for Youngster"[120].

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

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

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

120 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)[121], 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[122].

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

121 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)

122 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.[123]	
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 ☐	

[123] 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.[124]

[124] 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: 10 oct. 2014	**4. Case number: N/A**

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