Dublin Rape Crisis Centre

Response to the Committee on Justice and Equality concerning the issues of Online Harassment, Harmful Communications and Related Offences

September 2019

The Dublin Rape Crisis Centre (DRCC) is pleased to provide comment to the Committee on Justice and Equality for their examination of the issues of Online Harassment, Harmful Communications and Related Offences.

Introduction

The Dublin Rape Crisis Centre (DRCC) is a non-governmental organisation which aims to prevent the harm and heal the trauma of rape and sexual abuse in Ireland. DRCC is the largest of the 16 Rape Crisis Centres in the country. DRCC run the National 24-Hour Helpline which takes over 270 calls on average each week from victim/survivors of sexual violence and their supporters. DRCC provides face to face therapy for nearly 600 people a year. DRCC also provides training for about 2,000 people, including those working on the frontline with victim/survivors of sexual violence and those working with children and young people.[1] DRCC personnel accompany victim/survivors to the Rotunda Sexual Assault Treatment Unit (SATU), to Garda Stations and to court. DRCC advocates on behalf of victims/survivors and carries out public awareness campaigns to prevent sexual violence.

In our work, we see the often life-long consequences of the trauma and harm caused by sexual violence of all kinds. We also know from our experience that often times this harm is as a result of technology that is used to harass and humiliate.

We have structured our responses to the Committee in the form of answers to the questions set out in the issue paper.

Definition of communication in legislation

1. There are currently significant gaps in legislation with regard to harassment and newer, more modern forms of communication. Is there a need to expand the definition of 'communications' to included online and digital communications tools such as WhatsApp, Facebook, Snapchat, etc. when addressing crimes of bullying and harassment?

DRCC recommends broadening the definition of communications to cover all digital and electronic images and forms as well as written and spoken words so that communications sent in online format are covered by law, which is currently not the case. This is in line with the recommendation of the Law Reform Commission's 2016 Report.[2]

[1] See DRCC Annual Report 2018, https://www.drcc.ie/wp-content/uploads/2019/07/FINAL-DRCC-Annual-Report-2018-D4.pdf.

[2] Law Reform Commission (2016): https://www.lawreform.ie/_fileupload/Reports/Full%20Colour%20Cover%20Report%20on%20Harmful%20Communications%20and%20Digital%20Safety.pdf.

In order to provide clarity as to the scope of the offence, Section 10 of the Non-Fatal Offences Against the Persons Act 1997 should be amended to apply to all forms of communication including through digital and online communications when addressing the crimes of bullying and harassment.

2. What lessons can be learned from models used in other jurisdictions such as the UK, New Zealand and other European countries where legislation is now in place to address these issues? How do we establish an appropriate model without compromising free speech?

Many jurisdictions have laws in place protecting people from online sexual violence. The offences introduced in Australia,[3] New Zealand,[4] England and Wales[5] to target online harassment and harmful communications focus both on **the behaviour** and on **the impact of such behaviour**.

Therefore, we would recommend that harmful content be defined as any content that seriously interferes with the peace and privacy of the other person or causes alarm, distress or harm to the other person. This is similar to the definition set out in the Australian Enhancing Online Safety Act of 2015, where the Office for the eSafety Commissioner defined harmful content as *'content which is seriously threatening, seriously intimidating, seriously harassing or seriously humiliating'*. In New Zealand's Harmful Digital Communications Act of 2015, harm is defined as '*serious emotional distress'*.

Freedom of expression is not an absolute right and must be balanced against the harm caused by online harmful communications. Currently, our existing criminal legislation on this issue is entirely inadequate to address issues of harassment, stalking, voyeurism or other harmful online behaviour and does not protect the rights of those who are victims of it. If the definition of harmful content outlined in the previous paragraph, or a variation of that, is adopted, then there would be a more balanced approach which would not impose undue restrictions on the right of freedom of expression which only requires the removal of content when the content is injurious to the victim.

The Law Reform Commission's 2016 Report[6] outlines the extent of the right of freedom of expression in Ireland but also notes the need to balance this against the right to privacy. It also refers to the European Court of Human Rights, and the incorporation of the European Convention on Human Rights into Irish law.[7] Recent jurisprudence of the European Court of Human Rights (ECHR) has also noted the need to balance rights in the context of the right of freedom of expression.

[3] Enhancing Online Safety Act 2015: https://www.esafety.gov.au/about-the-office/legislation.
[4] Harmful Communications Act 2015: http://www.legislation.govt.nz/bill/government/2013/0168/latest/whole.html.
[5] Protection from Harassment Act 1997 as amended by the Protection of Freedoms Act 2012: https://www.cps.gov.uk/legal-guidance/stalking-and-harassment.
[6] Law Reform Commission Report 2016: See para 1.43ff supra.
[7] European Convention on Human Rights Act 2003.

3. How do we ensure that any legislation that is enacted is flexible enough to keep up with changing and advancing technologies, new apps and other online forums, including the more familiar social media sites?

The Law Reform Commission Report 2016 refers to the principle of technology neutrality but points out that while the same laws should apply online as offline, this does not necessarily mean that identical solutions are going to work for the two types of communication.[8]

DRCC recommends a flexible approach whereby the legislation would be supported by capacity for a Digital Safety Commissioner to regulate content within the main mandate of the legislation. The Commissioner would have mandatory powers to implement the legislation, capacity to build codes of practice and the like, and issue take-down notices or other appropriate sanctions. Based on the data and research of that office, rules could be adjusted to ensure that the legislation was effective and current.

Harassment, stalking & other forms of online abuse

4. Online harassment can take the form of non-consensual taking and distribution of intimate images or videos, otherwise known as 'revenge porn', 'upskirting', 'downblousing' and other forms of sharing of imagery online without consent. What approaches are taken to addressing these issues in other jurisdictions?

These forms of non-consensual sharing of intimate images are recognised as specific criminal offences in other jurisdictions.

In England and Wales, the Criminal Justice and Courts Act 2015[9] deals with the disclosure of private sexual images with the intention to cause distress. So-called '*upskirting*' is a specific criminal offence in England and Wales, punishable by up to two years' imprisonment.[10]

New Zealand has similar legislation to England and Wales, where they too created a specific offence of '*filming from beneath or under a person's clothing*'.[11]

[8] Law Reform Commission Report 2016: See para. 1.83 ff supra.
[9] http://www.legislation.gov.uk/ukpga/2015/2/section/33/enacted#section-33-1
[10] The Voyeurism (Offences) Act 2019 http://www.legislation.gov.uk/ukpga/2019/2/contents/enacted The 2019 Act criminalises someone who operates equipment or records an image under another person's clothing, without that person's consent or a reasonable belief in their consent and where the purpose is to obtain sexual gratification or to cause humiliation, distress or alarm.
[11] Sections 216G-N of the New Zealand Crimes Act 1961 (as amended by the Crimes (Intimate Covert Filming) Amendment Act 2006). Section 216G defines "*intimate visual recording*" to include recordings of:
"*a person's naked or undergarment-clad genitals, pubic area, buttocks or female breasts which is made:*
(i) from beneath or under a person's clothing; or
(*ii) through a person's outer clothing in circumstances where it is unreasonable to do so."*
195 Sections 216J (prohibition on publishing, importing, exporting or selling intimate visual recording) of the New Zealand Crimes Act 1961.

In Australia,[12] technology-facilitated stalking and abuse involving the use of technology such as the internet, social media, mobile phones, computers, and surveillance devices to stalk and perpetrate abuse on a person, is classed as criminal behaviour. Such behaviour includes:

- Making numerous and unwanted calls to a person's mobile phone;
- Sending threatening and/or abusive messages (text messaging, WhatsApp, Snapchat, Facebook messaging, Twitter);
- Hacking into a person's email or social media account to discover information about them;
- Hacking into a person's email or social media account to impersonate them and send abusive messages to family/friends of that person;
- Using surveillance devices to spy on a person;
- Using tracking devices to follow a person;
- Sharing, or threatening to share, intimate pictures of a person.

The Canadian Criminal Code provides that any person who '*knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of another person knowing the person depicted in the image did not consent, or being reckless as to this, is guilty of an offence'*. In Canada, there is an exemption whereby no offence will be committed 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*'.[13]

In Scotland, it is an offence under the 2016 Act[14] to disclose or threaten to disclose an intimate photograph or film. In England, the *mens rea* required is intent, however, in Scotland the law goes broader and includes recklessness.

In Canada, Australia, England and Wales there is a privacy test. In Canada, the definition of intimate images contains a reasonable expectation of privacy requirement.

With the Australian offence, the court must take into account the degree to which distribution affected the privacy of the person depicted in the image.

In the English offence, there was a requirement that the image or film be private, which is defined as something that is not of a kind ordinarily seen in public.

5. New offences are proposed to cover these issues in Deputy Brendan Howlin's Private Members Bill on this subject. Is the creation of new offences necessary or is existing legislation sufficient? Should other forms of image-sharing issues – such as exposure - also be addressed?

Current legislation in Ireland appears to be insufficient to capture these crimes as they are rarely prosecuted. Harassment requires a pattern of behaviour to be prosecuted. A single

[12] http://www.dvrcv.org.au/sites/default/files/ReCharge-Legal-Guide-VIC-Criminal-Offences.pdf

[13] Section 162.1(3) of the Canadian Criminal Code.

[14] Abusive Behaviour and Sexual Harm (Scotland) Act 2016 http://www.legislation.gov.uk/asp/2016/22/contents/enacted.

image uploaded to the internet without consent can cause devastating consequences for the person whose image is uploaded. Current stalking legislation is insufficient to address online stalking. Other forms of non-consensual image theft and covert or overt sharing are not covered by Irish law as it stands.

6. What kind of oversight and regulation of online service providers is possible/used in other jurisdictions? Currently, online providers are self-regulated. Is a proactive, self-regulating approach from online companies to activities such as revenge porn and other forms of harassment preferable to the creation of more laws?

While Minister Bruton has announced that a Digital Safety Office and Commissioner is to be established, none exists at this time. It is crucial that consideration of the issues in this submission take into account the development of such an office and Commissioner for Digital Safety as it should play a central role in oversight and regulation of online service providers.

In addition to the power to prosecute harmful behaviour discussed above, we recommend a notice and take-down system operated by the office of Digital Safety. Under this system, we recommend that the user first be required to make their complaint directly to the relevant digital service undertaking. Then, if the content is not taken down or a notice not complied with in a take-down timeline specified in a code of practice, then the user should have access to a complaint mechanism to the Commissioner. The digital service undertaking would thus be the first port of call and the Digital Safety Commissioner would be an appeal body only. In addition, there should be a system of mediation whereby there is an option, if both parties consent, to discuss whether or not the content should be removed.

The regulator's take-down procedure could follow a two-tiered system, similar to the model in Australia. Using this approach, digital service platforms would be divided into two categories. The first category could be intended for smaller digital service platforms, that have implemented certain basic online safety requirements, which could be set out in legislation, as has been done in Australia. The second category would be intended for larger digital service platforms. A tier one social media service may be **requested** by the Commissioner to remove harmful content for, while a tier 2 social media service may be given a notice (a social media service notice) **requiring** the removal from the service of harmful content. In addition, it could be advisable that a regulator also has the power to require a person who posts harmful content to remove such content. These notices requiring the removal of content should also be enforceable by the courts. For this procedure, it would be advisable that the Digital Safety Commissioner develop a code or codes of practice, similar to that outlined by the Law Reform Commission in its 2016 report.

7. Is any data provided by online service providers in relation to the reporting or prevalence of activities such as upskirting/revenge porn/cyberbullying and other online behaviour that can be used to develop and draft future legislation?

Not to our knowledge.

8. To what extent are An Garda Síochána equipped and resourced to deal with the issues arising from harmful online communications such as these?

An Garda Síochána is insufficiently equipped and resourced to deal with these issues. It is partly hampered by the lack of adequate legislation. The Commission on the Future of Policing identified [15] the need to for An Garda Siochána to build its cyber capacity. Personnel need to be trained and allocated specifically to investigate this type of crime. They also need further powers of discovery and seizure of material from internet companies.

While the Gardaí will continue to be responsible for investigating and prosecuting these offences, it is important that platforms take preventative steps to protect victims of such offences.

9. Should 'cyberstalking' be treated as a separate offence to online harassment? What constitutes stalking-type behaviour online? Is there a need to legislative specifically for this activity?

Online harassment, sometimes referred to as "cyberharassment," usually pertains to threatening or harassing emails, instant messages, or website entries. It is often repeated attempts to target a specific person by directly contacting them, or indirectly using or disseminating their personal information, causing them distress, fear, or anger.

Cyberstalking involves using the Internet or other electronic means to stalk a victim, and generally refers to a pattern of threatening or malicious behaviours. To be considered cyberstalking, the behaviour must pose a credible threat of harm to the victim.

We would recommend that cyberstalking should be legislated for specifically and recommend the findings and proposals of the Law Reform Commission Report 2016 in relation to this.

10. Based on the findings of other jurisdictions such as in the UK, An Garda Síochána will require consistent training in order to maintain an appropriate level of knowledge with regard to indictable behaviours. Are resources available for this?

Not at the moment. See response to Question No.8 above.

15 http://www.policereform.ie/en/POLREF/The%20Future%20of%20Policing%20in%20Ireland(web).pdf/Files/The%20Future%20of%20Policing%20in%20Ireland(web).pdf See paras 20-24.

11. Fake accounts/troll accounts used to harass or target others with abuse – what measures can be taken in relation to these without effecting freedom of expression?

There would be a substantial increase in safety, a reduction in crime and much more responsibility online if every account had a verified author. This is not the current model for online companies but would be a substantial safeguard against criminal behaviour and activity (such as that on online dating sites), against defamation (trolls and fake accounts across social media) and irresponsible posting. Companies would be responsible for verifying. Posters/ authors would be responsible for criminal activity, defamation and harmful communications. This should be universal but could at least be Europe-wide with EU involvement.

12. Do other jurisdictions have statutory measures to protect victim identities in cases of online harassment being released online post hearings, etc.?

Hopefully our previous responses have dealt with this.

Harmful online behaviour and young people

13. How do we most appropriately regulate social media platforms to prevent cyberbullying and inappropriate sharing of personal images?

Online platforms are already required to remove content that is a criminal offence under Irish and EU law, such as material containing incitement to violence or hatred, content containing public provocation to commit a terrorist offence, offences concerning child sexual abuse material, or content concerning racism and xenophobia.

In addition, see response to Question No. 6.

14. For young people who participate in such online behaviour as consensual image sharing, how can it be ensured that they are not inadvertently criminalised when legislation is enacted? What safeguards can be put in place?

Recent reports have highlighted the dangers for children growing up today and their exposure to an unprecedented level of harmful communications.[16, 17]

The principle of proportionality referenced in the Law Reform Commission 2016 report is relevant in this response and in response to the next question. As it outlines, a "*hierarchical approach is also necessary within this area because this type of harmful communication often involves children and young people who require a less coercive response because of their immaturity. The immaturity of young people may exacerbate the online disinhibition*

[16] https://cybersafeireland.org/media/1300/csi_annual_report_2018_w.pdf.
[17] *Cyber safety is the child protection issue of our time'* warns the ISPCC: https://www.siliconrepublic.com/life/ispcc-cyber-safety-child-protection.

effect leading to a greater level of impulsive behaviour among young people compared to adults. These factors mean that it would be impossible, as well as undesirable, for all harmful digital communications to be dealt with by the criminal law or perhaps even the civil law, and that a threshold is therefore required before the law should be engaged."[18]

We propose that this proportional/ threshold approach be adopted. In addition, children and young people should receive adequate information and education in relation to harmful and healthy relationships. In this regard, the review of consent and healthy relationships being undertaken by the National Council for Curriculum Assessment is relevant.

15. Deputy Brendan Howlin's Private Members Bill provides that those under 17 should not be fined/imprisoned but put into relevant education or supports. Would these supports be part of the same educational supports offered to all young people/schools or would they be a separate entity? Are current supports being utilised? Are there sufficient resources to provide for such a provision when enacted?

See response to question No. 14.

[18] Law Reform Commission Report 2016, para. 1.77 ff supra.