Seminar report

Building Effective Responses to Cyberviolence Against Women

Niall Crowley

ABOUT

This report summarises the SAAGE hybrid seminar held on 18 June 2024 in Brussels.

Fondazione Giacomo Brodolini S.r.l. SB (FGB SRL SB) is an Italian independent research centre inspired by the principles of labour and social inclusion, gender equality, cultural diversity and respect for fundamental human rights, welfare promotion, territorial cohesion, sustainability, and technological innovation to boost economic growth, attention to the environment, access to employment through new skills, and participation for local development.

SAAGE activities and products are financed by and prepared for the use of the European Commission, DG Justice, Consumers and Gender Equality; Unit D3 'Gender equality', in the framework of a contract managed by FGB Srl SB. It does not necessarily reflect the opinion or position of the European Commission or of the DG Justice, Consumers and Gender Equality; and nor is any person acting on their behalf responsible for the use that might be made of the information therein contained.

TABLE OF CONTENTS

INTRODUCTION

Katja Lenzing, Deputy Head of Unit, Gender Equality Unit of DG JUST, European Commission, opened the seminar with an introduction to the current context for the European Commission in this policy field.

The digital space is a vital part of our lives, offering advantages and opportunities but also presenting risks. Women are at particular risk of cyberviolence. This can lead to self-censorship by women, their withdrawal from the digital space, and absence from the online debates. As such, the Gender Equality Strategy 2020-2025 of the European Commission has been concerned with equality in the digital space.
Most recently, in this regard, the European Directive on combating violence against women and domestic violence was adopted in May of this year, with Member States having three years to implement this. This criminalises the most common forms of cyberviolence and is also concerned with prevention, protection, support and access to justice. Specifically there are obligations posed on Member States in relation to: developing digital literacy skills and critical thinking; making provision for online reporting of cyberviolence; and requiring online platforms to remove illegal content.
Going beyond the Directive, the European Commission is working with online platforms on a voluntary framework for the protection of women from cyberviolence, developing a code of practice in this regard.

KEYNOTE ADDRESS

Professor Kim Barker, Professor of Law, University of Lincoln, United Kingdom, and Director of the Observatory on Online Violence Against Women, presented an overview perspective on 'Online Violence against Women: forms, spaces, tools, perpetrators, impact and the requirements for an effective response'.

Cyberviolence is an issue that evolves and grows as technology evolves. As such there is a particular challenge to engage with the development of the technology and advance equality by design in this field. Cyberviolence involves a spectrum of behaviours and takes a wide range of forms, in effect a continuum of violence. Some forms are criminalised, and some are harmful but deemed legal. There is a challenge to establish what is legally actionable and a need to be specific about the acts involved. There is a multiplicity of different terms for these acts and while there is some categorisation there is limited agreement on terminology.
All spaces need to be a focus for attention, going beyond social media, as anywhere a person can be reached by internet-connected means is a space where online violence against women can be experienced and perpetrated. Perpetrators also need to be a focus for attention. Some are organised around high profile women, but perpetrators can be anyone, including adults and children. Often they are unknown and anonymous, but not always and platforms can also identify perpetrators. There are repeat perpetrators operating across platforms. It is possible the abuse is accidental and not intended, but it remains a challenge.
Cyberviolence is extremely harmful and hugely significant for women, as online abuse can quickly proliferate and spread, with each level reached triggering greater levels of harm. Women can be silenced and can withdraw from digital spaces, social and psychological harm can accrue for women, and their participation in political and public life can be curtailed. There is an intersectional dimension with other characteristics brought into play alongside that of gender.
Looking forward: There is a need to ensure a gendered response to what is a gendered problem. There is legal recognition for the issue, but gender neutrality in legal provisions needs to be addressed. Legal

consideration needs to be given as to what forms of cyberviolence can be criminalised. Investigation and prosecution needs to be victim centred and gender sensitive and it needs to be resourced and to be based on best practice guidance. Perpetrators need to be held accountable with appropriate sanctions. Victims need support and protection from any reprisals. Multi-stakeholder involvement is needed with: online platforms taking responsibility for the issue as they can easily identify perpetrators; a focus on this issue in education; and investment in digital literacy

The subsequent discussion explored a gender-sensitive response as needing to include a focus on policy with a gendered focus; a victim support package that includes for safe spaces, access to a woman police officer, appropriate psychological support and counselling, legal assistance, and a focus on what outcome the woman wants from the process; and police training.

A key challenge lies in changing the culture and responses of the bigger actors in this field (e.g. platforms) as there is a mirroring that can happen where change online affects change in society and vice-versa. Working with platforms is, therefore, important.

There is a challenge as to how much power should be given to the authorities to monitor the situation in a context where we have already gone too far in giving away our personal data. Digital literacy training needs to address privacy and what one actually is consenting to in signing up to online activity. There is a need to find different ways of informing people as to what they are consenting to in a context where the current methods present limitations.

The legislative process is slow and technology advances with speed, so future proofing legislation is difficult. An overarching legislative framework is needed with small updated legislative elements easier to agree with speed. This would involve a core of principles that should not change over time despite technological changes and a second part that should track and be responsive to technology evolution.

There is a need to deal with the behaviours and perspectives in the real world that underpin cyberviolence against women, in a context where addressing the technology is challenging.

FORMS OF CYBERVIOLENCE

Professor Elena Martellozzo, Criminologist at Middlesex University and Associate Director for the Centre of Abuse and Trauma Studies (CATS), United Kingdom, presented on 'Exposing Online Pornography as Cyber Violence Against Women and Girls: Understanding the Dangers and Evaluating Its Consequences'.

The digital space offers many positives for young people, though it also holds vulnerability in exposure to harmful persons, in terms of grooming, coercion and exploitation, and in exposure to harmful content in terms of pornography, violence, and child abuse material. Looking to the issue of pornography, it is there and it will be there in a context of huge demand. It won't be eradicated and we need to see where we can make a difference. In this, there is a need to ensure children do not get access.

Pornography is a powerful industry, bigger than Netflix or Hollywood. This is an industry that thrives on anonymity and ease of access. In the words of one child research participant, it is harder to avoid it than to find it. The best-selling pornography videos are found to contain high levels of physical and verbal aggression, where the perpetrators are male and the targets are female, and where the targets show pleasure at or neutrality in responding to the aggression. This is problematic where pornography is the most prominent sexuality educator for many young people, and most young people discover pornography before they encounter sex.

Research in the UK has shown that, of a sample of over 2,000 children, 56% of boys have viewed online pornography, feel positive about pornography and are less likely to see pornography as exploitative degrading, and humiliating; and 40% of girls have viewed online pornography, feel more negative about pornography and worry about the expectations boys who have viewed pornography might have of them as girls. Among 11-12 year olds 28% have viewed pornography and 21% want to copy it, among 13-14 year

olds 46% have viewed pornography and 39% want to copy it, and among 15-16 year olds 65% have viewed pornography and 42% want to copy it. The reaction on first viewing of pornography is principally characterised by curiosity, shock, confusion, disgust and nervousness, but the reaction following repeated viewing over time is principally characterised by being turned on by it.
Research participants, the voice of children, point to the need to foster safe, secure online engagement; provide secure and private virtual and real spaces for young people to have conversations about the issues; provide specialist training for age and gender appropriate sessions on the issues to be facilitated; co-create learning spaces with young people; support children in ways that acknowledge their socio-sexual development; and support those troubled by their online experience.
Looking forward: In progressing change, there is a need to create safe spaces for disclosure about use of pornography; continue research into the issue including in relation to types of pornography that need to come under a legal remit, and to site moderation processes; enhance age verification on sites; increase warnings as to relevant laws; enhance reporting functions; and provide more information in schools around the legislative and wellbeing risks. Good practice in Australia was noted in this regard, with a model for discussing pornography in schools that involves pupils, parents and teachers.
The subsequent discussion noted age verification was challenging to implement. Increased warnings about content could usefully come in the form of nuggets or as part of a process that provides for and enables reflection.
The need to view pornography only as one of the many causes of aggressive behaviour was noted. The role of pornography as a repackaging of the social conditioning we have always been faced with in relation to gender was noted.
The impacts of online pornography in being the introduction to sex for young people need to be explored in terms of young people becoming nervous, worried and fearful and not having the positive experiences they should have, rather than in terms of fears about bringing up a new generation of perpetrators.
The importance of having conversations with young people in this regard was noted, with an emphasis on the role of schools in this, though some parents can block this, and some schools can refuse to accept this as an issue for their pupils.
The role of NGOs working on these and linked issues was noted as important in giving space for children in this regard, and in shaping the discourse on the issues of sexuality for children. These organisations could be supported in their efforts.

Professor Chara Bakalis, Associate Professor, Deputy Head (Strategy and Development), School of Law and Social Sciences, Oxford Brookes University, Oxford, United Kingdom, presented on 'Addressing cyberhate as a form of cyberviolence against women'.

There is a continuum of online misogynistic hate speech. All forms of these degrade and essentialise women, and some openly call to physical violence, normalise rape and rape culture and sexual violence. All are potentially harmful, but policy and legal approaches need to differ for the different forms.
There is an impact from online misogynistic hate speech on individual women. Such hate speech affects the subconscious, how you see the world. It normalises harmful stereotypes. There is an impact from online misogynistic hate speech on society, as a lot of the abuse is about women in general and the online environment is toxic for women. There is an impact on bystanders. Such hate speech can also radicalise offline behaviour. There is an impact on democracy and political life as online misogynistic hate speech silences women and blocks their online participation and targets and discourages female politicians, in particular Black women politicians. Journalists too can avoid stories for the backlash they might generate.
In responding to this, there is a need to distinguish between hate crime, where a criminal offence is exacerbated by a hate element, and hate speech, where the offence is the hate speech itself. In addressing hate crime, it is important to ensure that there is: effective legal provision for an online and offline criminal offence in place; an effective regime in place that includes sex/gender as a protected characteristic; training for police and prosecutors; reporting systems; and engagement with social media companies and a requirement on them to remove material.

In addressing hate speech, freedom of expression comes into play and this means that only the most extreme examples can be criminalised, such as the promotion of hatred. Traditional policy responses are ineffective in the context of the sheer volume of online hate speech. Dissemination algorithms used by platforms are often the key problem and need to be a focus for action rather than the speech itself and, as such, there is a need to hold social media platforms to account.
Progress is being made with new legislation and its effective implementation will be important. The Digital Services Act requires removal of illegal material, but this needs harmonisation of hate speech laws across different jurisdictions as platforms work across borders. There is a risk assessment requirement that should involve some algorithmic oversight. In the UK, the Online Safety Act 2023 follows a similar approach with higher level duties for those under 18.
Looking forward: The focus needs to be on: harmful material, not necessarily criminalisation; dissemination limitation rather than content moderation; and education and other non-legal means of intervention.
The subsequent discussion explored the challenges in and the need for a focus on implementing the new legislation to achieve progress, with a need to invest in a regulator to monitor the online platforms.
The potential in a focus on dissemination, addressing the algorithms that push ever more extreme material on people, to allow for freedom of speech concerns was noted. The need for more regulation was suggested.

LEGAL ACTION TO COMBAT PORNOGRAPHY AS CYBERVIOLENCE

Dr. Karolina Mania, Ph.D in Law, Assistant Professor, Department of Strategic Management, Institute of Economics, Finance and Management, Faculty of Management and Social Communication, Jagiellonian University, Kraków, Poland, presented on 'Legal implications of revenge pornography and deep-fake pornography and possible responses'.

Deep-fake pornography is a new phenomenon that needs to be linked into the legal spheres, with consequences. There is a need for a proper definition of the phenomenon to serve this. Deep-fake pornography lies next to revenge pornography and belongs to the family of image-based sexual abuse and the non-consensual distribution of intimate images. It can be linked to a wide range of branches of the law: privacy law; defamation law; IP law; cybercrime; criminal law; civil rights; consumer protection law; employment law; family law; and contract law.
In the USA, 17 States have laws against deep-fake pornography. This is problematic in encompassing a wide variety of types of violation; penalties; and evidence requirements. Regulatory approaches differ, including: adding new specific regulation; updating privacy legislation; or updating the definition of child pornography in the context of AI used in that field. Revenge pornography laws differ in relation to intent and consent, leading to varying penalties. Laws that require disclosure and impose bans pose a challenge for victims in proving an 'illicit motive'. Few States apply the language of AI-generated images and some States imply that images must depict the victim's actual body parts, not AI-generated. Some States allow victim lawsuits, while others criminalise deep-fakes, which latter approach ensures victim anonymity.
There are examples of legal responses at national level in the EU, such as in Germany, France and the Netherlands, and in the UK. In the absence of specific legislation on deep-fake pornography, other legislation is deployed, in particular data protection and privacy legislation. However, it can be hard to establish the perpetrator, to prove the case and to compile applicable evidence.
Progress is being made at the EU level with the provisions in the AI Act, the Digital Services Act and the European Directive on combating violence against women and domestic violence. The immediate challenge is now focused on how such legislation will look like in practice, in terms of its transposition by Member

States and then in terms of its implementation.
Looking forward: Image-based sexual abuse and deep-fake pornography require legal definition and dedicated regulation. Identification systems need to be developed and deployed. There is a need to involve the Tech companies in responding to these issues including in relation to these identification systems. An inter-disciplinary approach and international cooperation are required for an effective response.
The subsequent discussion focused on the developments that have taken place at EU level and the challenge to ensure such developments have an impact in their implementation at Member State level. Effectiveness and good practice are key in the response at this level.
The challenge to explore how we conceptualise harm in law was noted given the new ways that emerge in how harm is caused. There is a need to explain what harm is. This can range from how you feel to impacts on one's life and safety.

Professor Abhilash Nair, Associate Pro-Vice-Chancellor for Business Engagement and Innovation & Associate Professor of Internet Law, University of Exeter, United Kingdom, presented on 'The Challenges in Regulating Internet Pornography'.

New models of intervention are needed in a context where regulation of adult pornography has not worked. Regulatory perspectives encompass: morality in terms of depravity and corruption; feminism in terms of objectification and degrading of women; civil libertarian in terms of freedom of expression; laissez faire in terms of the imperative of the market; and child protection. In many countries, regulation of adult content is generally focused on restricting publication/distribution in the particular country.
The complexity in regulating adult pornography arises from this issue falling under the framework of freedom of speech. While, as a result, adult pornography is legal in many jurisdictions, pornography that falls within the boundaries of obscenity can be outlawed. However, societies apply different levels of tolerance and different values in relation to acceptability. Where legislation is in place, challenges of enforcement also arise.
Transposing traditional legislative approaches to cyperspace, based on an obscenity standard, has not worked. Adult pornography has remained largely unregulated on the internet for all practical purposes in the USA with the striking down of a series of legislative initiatives. Where regulation is focused on the publication of content, this presents a barrier to effectiveness, in that publication abroad can undermine it. Different rules end up applying for domestic (small) content providers and international (large) providers.
There needs to be a shift in focus to restriction of children's access. The challenge is to keep children from accessing adult content intended for adults. A concern to keep children away from harm, however, faces difficulties of ascertaining the age of users. There are further difficulties in the absence of any harmonised approach as to the scope and definition of harmful content that could impair the physical, mental and moral development of children.
The specific requirements of individual Member States need to be catered for when it comes to technical approaches to age verification. There is an issue of lack of guidance as to how to implement age verification with few tools available. Some countries, like Germany and France, have issued age verification criteria to protect minors and established guidance for providers on how age verification should be implemented in practice, though this is currently more of an exception.
Recent developments of interest include: the Law of 30 July 2020 in France aimed at protecting victims of domestic violence which reaffirmed the obligations in relation to age verification (codified in Art 227-24 of the French Criminal Code). This criminalises the publication of pornography if minors can access it (self – declaration is not enough). The Audiovisual and Digital Communication Regulatory Authority can issue orders requiring compliance, failing which it can approach the court to block the sites. In the United States there are a variety of age verification requirements in legislation across a number of states. The Online Safety Act 2023 in the UK requires different levels of age assurance/verification.
Looking forward: The measures adopted to protect children, whether it is age rating or labelling, parental control systems or age verification tools that provide higher levels of assurance, should depend on the content and risk of harm it may cause. Guidance is required on this from regulators. Technical measures

adopted should be proportionate to the potential harm of the material. It is not envisaged that all content should be subject to age verification.

The euConsent mapping project identified that legislation is only the first step, and for the law to work, it also needs to have an effective enforcement mechanism. Age verification should not be seen as a one-stop-shop solution for protecting minors from harmful content. It is not a substitute for responsible parenting, or the myriad of legislation and other safeguards that are currently in place to protect children. While age verification tools have a key role to play in protecting children from harmful online content, services and products, these tools should respect children's rights and they should be privacy-preserving.

The subsequent discussion raised the issue of cultural values and whether the approach is about the cultural management of content or about being culturally neutral in a context where there is no single norm.

The use of an age limit is noted as a compromise as it is difficult to set in a context where growing up and cognitive development is a complex process that differs for different individuals.

It was noted that while age verification is important, pornography is not good for society and poses risks for women. It was suggested that good standards are needed for adult content providers with co-regulation in place to implement them. Harmful pornography needs to be addressed, and the accessibility of pornography to children under 18 needs to addressed. There is a need noted to avoid alienation and to have conversations with the pornography industry about this.