When Technology Meets Misogyny

Multi-level, Intersectional Solutions to Digital Gender-Based Violence

GEN POL
Gender & Policy Insights

Foreword

by Dr Lilia Giugni, GenPol CEO

Questions surrounding the politics of digitalisation are amongst the most profound of our age. Are digital technologies oppressive or emancipatory? And those of us who identify as feminists and fight for gender equality, should we side with techno-phobes or tech-enthusiasts? At GenPol, we celebrate the opportunities that digitalisation has opened up for women, vulnerable groups and social justice movements worldwide, but passionately believe that the ways in which technology reinforces the oppression of women should be investigated, denounced and addressed.

This paper is the result of a year of work, which has seen us working with digital gender-based violence survivors, experts and practitioners from different organisations and across different countries. Starting with the project launch event at the European Parliament in November 2018, we took to heart the call issued, among others, by the United Nations, Council of Europe and European Institute for Gender Equality to produce further, meaningful research on online violence against women. In particular, we felt that the best way we could contribute to the work of those who fight digital abuse on a daily basis was to retrieve existing good practices, analysing their strengths, possible drawbacks, transferability and scalability potential.

Like any form of violence and complex social problem, online attacks on women can only be addressed through a multi-level approach. We thus focused on case studies that range from legal interventions to educational projects, from cross-sector partnerships to the creation of brand-new advocacy organisations and software-based solutions, from the creative use of resources within established charities to grassroots campaigns and novel forms of in-depth reporting. We also made sure that the voices and needs of survivors of gender-based violence, and of the groups that are particularly exposed to the risk of experiencing it, were central to our research, final recommendations and advocacy efforts. It is above all to them, that this paper and our daily work at GenPol are dedicated.

Happy reading!

Lilia Giugni

Executive Summary

Our approach to DGBV. In this paper, we look at digital gender-based violence as a specific and particularly **pernicious form of abuse against women**, and explore multi-level solutions to tackle this.

Whilst online vitriol can be directed against people of all genders, existing research indicates that women's experiences online are qualitatively and quantitatively different. Not only are women worldwide more likely than men to be attacked on the Internet, but the digital abuse they face is also specific in its nature, as it tends to be **extremely sexualised and overtly motivated by gender[1]**. At the same time, the **effects of digital violence** are comparable to those of sexual and domestic abuse, in terms of both physical and mental health repercussions and impact on the professional and social spheres. We also have clear evidence that **sexist, racist, homo and transphobic abuse** and other forms of bigotry constantly intersect, online as offline, with heavy consequences on the lives of non-white, queer, disabled and poor women. With this in mind, we consciously use the term DGBV (as opposed to cyber bullying, trolling, or virtual violence) to create awareness around both the gendered nature of the phenomenon, and its extremely serious impact.

While recent studies have usefully mapped the problem and its ramifications, our review of academic and policy literature on the scope, causes and effects of DGBV highlighted that a focus on concrete solutions and good practices is now needed. With this in mind, we identify insightful **case studies extrapolated from different sectors, countries and levels of analysis**, and make **recommendations** based on a thorough analysis of the various practices' **strengths, potential drawbacks, and transferability** potential.

Our case studies. Scrutinising **Australia's recent legislation on image-based abuse**, we examined how **new laws** can successfully contribute to prevent and sanction a particularly invasive form of DGBV, which existing legal instruments were not able to capture. We also consider the advantages of particular **legal definitions** and understandings, and the **limits of standalone policy reform.**

In our second case, we investigated how a transnational women's organisation, **European Women's Lobby** (EWL), partnered with Google on a DGBV-related project. We treat this as a case of **cross-sector partnership**, analysing from EWL's perspective the benefits of the collaboration. While focusing on lessons to be learned for other **research and advocacy** initiatives aimed at mainstreaming feminist concerns into the tech industry, we also reflect on the **risks** to be mindful of.

---

[1] See, for example, Juhasz B, Pap E., Backlash in Gender Equality and Women's and girls' rights, Brussels, 2018; UN Women, Violence against women in politics, Expert Group Meeting Report & Recommendations, 2018; Atalanta, (Anti)Social Media. The benefits and pitfalls of digital for female politicians, 2018.

Our third and fourth cases, both from the **United Kingdom**, provide insights into the complementary benefits and drawbacks of two different strategies for **awareness raising, training and educational efforts**. We looked at **Childnet**, an **established charity** from the field of digital safety and children's rights, which developed **gender-sensitive projects** and used its existing resources and social capital to bring DGBV to the attention of its beneficiaries and target audiences. On the other hand, we illustrated the trajectory of **Glitch!**, a **single issue advocacy organisation** specifically created to educate the public, and to lobby policy makers and tech companies on DGBV and racist online abuse.

Finally, we focused on a case of **survivor-centred in-depth reporting** and on **the most interesting software-based solutions** in the field of online content moderation and DGBV reporting mechanisms. Our fifth case study considered a Romanian research project that blended **journalistic investigation, grassroots educational work, and political lobbying** surrounding DGBV issues. Our examination of different moderation options, instead, took into account both the impact of different policies and tools on **tech company employees**, and the risk that **AI instruments** may concur to perpetuate existing gender biases.

Our recommendations. Based on our analysis, our final recommendations touch upon the potential for both policy and legal intervention and target different stakeholders. We suggest that **new legislation** is needed to address specific legal loopholes and sanction instances of abuse uncovered by previous legislation (as in the case of image-based abuse). However, since **many existing provisions** on stalking, hate crimes, threats and privacy can apply to DGBV cases, we propose that **training legal and law enforcement personnel** to recognise the gendered and intersectional nature of the phenomenon is of the utmost importance. We also make a case for lawmakers to **push tech companies** to adopt more effective reporting mechanisms, take down procedures and moderation techniques, and for **introducing DGBV-related concerns into educational curricula**. Similarly, considering that we increasingly witness instances of DGBV in the workplace, we recommend that **training on digital rights and self-care** is provided by employers and professional associations for different categories of professionals and organisations, especially for those in public facing role. We pay specific attention to **gender equality training in the tech and media industry and academia**. Finally, we offer suggestions regarding **cross-sector partnerships** and **co-creation of resources** on DGBV that may **involve academic institutions, private and third sector organisations**, and specifically consider the types of intervention more appropriate to support **DGBV survivors, educators and practitioners**.

Table of Contents

List of authors

Dr Lilia Giugni is GenPol's CEO and works as a researcher at the University of Cambridge. She is a Fellow of the Royal Society of Arts, holds a PhD in Politics from Cambridge and sits in the board of several organisations in the gender equality space. Her research and advocacy work lie at the intersection between feminism, organisational studies, social justice and social innovation. Twitter: @liliagiugni

Chiara De Santis is GenPol's Chief Policy Officer and a consultant on international public policy. She has worked for the European Commission, the European Parliament, the United Nations, and has overseen several EU-funded projects. She holds a Bachelor's and two Master's degrees in Politics and International Relations and has researched matters of regionalism, foreign policy and gender.

Nathalie Greenfield is currently studying human rights law at Cornell Law School in NY, USA, where her focus area is gender-based violence. Prior to heading to the US, she worked in the European Parliament's Equality and Diversity Unit on gender equality policy in the EU. She has enjoyed being a Research Associate for GenPol since 2017. Twitter: @nath_greenfield

Venera Dimulescu is an independent journalist living in Bucharest. She is currently working as a culture and social reporter at Scena9 and Casa Jurnalistului publications. She has studied philosophy at the University of Bucharest and currently works as an independent researcher.

Ciara Taylor has been working with GenPol for a year as a research and communications intern. She is a Philosophy graduate from the University of Cambridge, specialising in political philosophy, ethics and gender studies. Her dissertation work focused on trans-inclusion within the feminist movement.

E. M. Wroth is a writer, researcher and educator. She is the recipient of an AHRC Collaborative Doctoral Award between Durham University and the Bowes Museum. Inspired by the #MeToo movement, her work Sex, Song and Self-fashioning: Women on the Popular Parisian Stage focuses on the influence of popular culture on gender politics, sexual conduct and notions of consent in modern Western discourses.

Ilaria Galizia is a medical doctor and a psychiatrist, with a keen interest in investigating the intersections between gender and mental health. She holds a Master's degree in Gender Studies and Politics, and wrote her dissertation on the impact of gender as a risk factor in depression cases. She is a member of Global Health 50/50 - Towards Gender Equality in Global Health.

Anna Yakovleva is dedicated to make contributions to the fight against global health inequalities. She is completing her PhD in Virology at Cambridge University, and is a contributor to the UK-based think tank Polygeia. Anna has worked for over a year as a GenPol Research Associate.

Mariana Plaza has worked for a year as a GenPol Research Intern. She is about to complete a degree in Politics, Philosophy and Law at King's College London. She is interested in how the legal system can serve as a mechanism to address inequality between men and women in society, and has interned and volunteered for several organisations in the gender and policy space.

Jushya Kumar recently graduated from SOAS, University of London, with a Master's degree in Globalisation and Development. She holds a Bachelor's degree in Sociology and has worked on various women-centred development projects — including matters of violence against women, child marriage and adolescent pregnancy, and an awareness campaign on menstrual hygiene in rural areas.

Sarah Awan is a Manager in Digital at PwC, having previously worked for a Microsoft consultancy and IBM. She recently completed a Master in Social Innovation at the University of Cambridge, where she was

awarded a 30% Club Scholarship and researched the intersections between gender and technology. She has worked with multiple girls' rights organisations including Plan International and Girl Rising.

Lily Rosengard is a feminist activist and researcher, working in multilateral and civil society partnerships for Plan International, a girls' rights' NGO. Lily is currently studying a part-time MA in human rights at UCL, after an undergraduate degree in philosophy and religious studies at the University of Cambridge.

Stella Rhode recently graduated from the University of Cambridge, defending a dissertation on sexual consent and power. She has particular interests in digital gender-based violence and epistemic injustice, and is currently living in Edinburgh.

Graphics, editing and media team

Chiara De Santis, GenPol Chief Policy Officer
Ellen Davis-Walker, GenPol Chief Communication Officer
Francesca Di Nuzzo, GenPol Chief Finance Officer
Nathalie Greenfield, GenPol Research Associate

About GenPol

GenPol - Gender & Policy Insights is a think tank consultancy and a social enterprise. GenPol advocates for gender equality, researches gender issues through an intersectional feminist lens and uses research findings to help others understand gender dynamics and find gender-sensitive solutions to social problems.

We believe that gender relations are key to understanding the complexities of the modern world and producing meaningful social change. Our research sheds light on matters of violence, politics, media, work, education, technology and social justice. Making gender analysis accessible and impactful beyond academia is crucial to our mission, and we regularly publish reports, briefs and policy recommendations, and raise awareness on gender equality matters through different media and live initiatives.

List of abbreviations

BAME: Black, Asian and Minority Ethnic
DGBV: digital gender-based violence
EIGE: European Institute for Gender Equality
EU: European Union
FRA: European Union Agency for Fundamental Rights
GDPR: General Data Protection Regulation
GBV: gender-based violence
IBA: image-based abuse
ICTs: information communication technologies
LGBTQ+:   Lesbians, Gays, Bisexual, Transgender, Queer and other gender identities and
               sexual orientations
MP: Member of Parliament
MEP: Member of European Parliament
UN: United Nations

Acknowledgements

Part 1

Tackling digital gender-based violence: the state of the art

Digital gender-based violence: the state of the art

By Lilia Giugni, Anna Yakovleva, Nathalie Greenfield, Ilaria Galizia, Ciara Taylor, Mariana Plaza, Stella Rhodes, Lily Rosengard, Jushya Kumar & Sarah Awan

1.1 Introduction: digitalisation through an intersectional feminist lens

Over the last decade, digital technologies have redesigned socio-economic, political and cultural processes in complex and often poorly understood ways. Specifically, **mobile information and communication technologies (ICTs)**, including different types of social media, have become for millions an indispensable tool and a part of daily life.

Our approach

At GenPol, we strongly believe in the value of examining social phenomena through an **intersectional feminist lens**, and question their implications and impact upon women, LGBTQ+ groups, migrants, BAME, disabled and economically vulnerable people and communities. As acknowledged by both academic and policy analysts[2], **democratic and fair digitalisation trends** may help reverse gender-based injustice and create opportunities for women, girls and other historically discriminated-against groups. To begin with, ICTs, and social media especially, have played a central role in the revitalisation of feminist, LGBTQ+ movements and other forms of mobilisation for social justice causes worldwide. By strengthening traditional forms of advocacy and awareness-raising work, they have enabled new generations of activists, together with individuals and groups situated at the periphery of decision-making arenas, to connect, communicate and organise[3]. Furthermore, tech-based solutions have emerged in the camps of education, public health, local governance, community entrepreneurship and social innovation, opening promising pathways for women and all those interested in truly inclusive and sustainable development[4].

On the other hand, we should not lose sight of **those who are excluded from, or harmed by, the digital revolution**. While the underrepresentation of women in STEM fields and the tech industry has long attracted public attention, the ways in which digitalisation may help perpetuate the oppression, exploitation and discrimination of women, minority ethnic

---

[2] See, for example, Wajcman, J., 'Feminist theories of technology' in Cambridge Journal of Economics, 34(1), pp.143-152, 2018; Plan International Briefing Paper: Digital Empowerment of Girls, 2018; Unesco, Global Education Monitoring Report, 2018; ITU, Gender Equality and the Empowerment of Women and Girls through ICTs, 2018, available at:
http://www.itu.int/en/action/gender-equality/Pages/default.aspx.

[3] For further details, see, for instance: Association for Progressive Communication, ICTs for Feminist Movement Building: Activist Toolkit, 2018, available at: https://www.apc.org/en/pubs/icts-feminist-movement-building-activist-toolkit; Cammaerts, B., ICT-usage among transnational social movements in the networked society - to organise, to mobilise and to debate, 2005, available at:
https://core.ac.uk/download/pdf/93297.pdf; Giugni, L., 'Women's Rights Backlash and Feminist Revival: Gender Equality in 2019', The Globe Post, 2019, available at: https://theglobepost.com/2019/04/12/gender-equality-2019/

[4] See European Parliament, Empowering women and girls in media and ICT - key for the future, 2018, available at http://www.europarl.europa.eu/RegData/etudes/PERI/2018/606788/IPOL_PERI(2018)606788_EN.pdf

groups and other vulnerable categories go deeper than the current conversation on representation may suggest. Not only do we witness a significant **gender gap in terms of Internet penetration and access to ICTs** – a global divide that is affected by socio-economic class, race and geography[5]. There is also evidence that Internet-based technologies are providing **novel tools and channels to physically, psychologically and economically harm women**, **exploit and control their bodies and work**, and deprive them of their political agency[6].

Our focus

In this paper, we specifically focus on **digital gender-based violence (DGBV)**, which we examine as a form of gender-based abuse[7]. In fact, whilst online vitriol and various typologies of cybercrimes and digital exploitation can be directed against people of all genders, previous research clearly indicates that **women (together with non-white, non-heterosexual, non-cisgender, disabled people) are disproportionately more exposed** to extreme online violence[8]. The violence that women face on the Internet is also specific in its nature, in the sense that it tends to be extremely sexualised and overtly **motivated by the victim's gender**. At the same time, as suggested by gender-based violence experts and practitioners internationally, it is hard to ignore that **online and offline violence** against women exist on a continuum, intersecting with and reinforcing one another[9]. In fact, ICTs are increasingly used by misogynistic groups, stalkers, abusive partners and other perpetrators to control and harass their victims. They also play a significant role in human trafficking, illegal pornography and other forms of sexual and gender-based organised exploitation. Moreover, it is rather telling that researchers identify in survivors[10] of DGBV

---

[5] See Web Foundation, Women's Rights Online Digital Gender Gap Audit, 2016, available at:
https://webfoundation.org/research/digital-gender-gap-audit/; USAID and US Global Development Lab, Closing the Digital Gender Gap, Available at:
https://www.usaid.gov/sites/default/files/closing_the_digital_gender_gap.pdf.

[6] See GenderIT.org: Feminist reflection on Internet policies, last accessed October 2019, available at:
http://www.genderit.org/.

[7] A vastly used definition of gender-based violence is provided by the European Institute for Gender Equality (EIGE) at: https://eige.europa.eu/gender-based-violence/what-is-gender-based-violence.

[8] See Pew Research Center, Online Harassment, 2014, available at:
http://www.pewinternet.org/2014/10/22/online-harassment/; Agency for Fundamental Rights (FRA), Violence against women: an EU-wide survey. Main results report, 2014, available at: http://fra.europa.eu/
en/publication/2014/violence-against-women-eu-wide- survey-main-results-report); Amnesty International, Toxic Twitter, a toxic place for women, 2018, available at:
https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/;
European Commission, 2018 Report on equality between women and men in the EU, 2018, available at:
http://ec.europa.eu/newsroom/just/document.cfm?doc_id=50074; Project DeSHAME, available at
https://www.childnet.com/our-projects/project-deshame/about-project-deshame

[9] See Kelly, L., 'The Continuum of Sexual Violence', in Hanmer, J., Maynard, M. (eds) Women, Violence and Social Control. Explorations in Sociology. Palgrave Macmillan: 1987; European Women's Lobby, Disrupting the continuum of violence against women and girls, 2017, available at:
https://www.womenlobby.org/IMG/pdf/facsheet_violence_against_women_and_girls_in_europe_2017_webs ite.pdf.

[10] In this paper, we use the notion of victim and survivor of gender-based violence interchangeably. We are aware that both present specific connotations in feminist analysis, as the former emphasises the reality of the harm suffered by a person and it is often used in legal dealings, while the latter focuses on recognising that

the **same symptoms** caused by forms of sexual and domestic abuse that traditionally took place offline, both in terms of physical and mental health impact and repercussions in the social and professional spheres[11].

Our paper

Building on these existing contributions, we are delighted to observe that – thanks to the efforts of activists, experts and survivors across many countries – in the last few years DGBV has gained centrality in policy, public and industry-specific discussions. Whilst this is an **important step forward**, we welcome, and attempt to respond to, the call for a stronger focus on **viable, evidence-based strategies** that was recently launched, among others, by the United Nations, OSCE and European Parliament[12]. Like all multifaceted social problems, DGBV has intricate causes and corollaries, and must be understood and addressed at multiple levels.

With this in mind, our paper seeks to **contribute to the conversation on DGBV and the future of digital work, policies and innovation** by offering **an examination of good practices** from different countries, fields and at various levels of analysis. By selecting and identifying insightful **case studies**, discussing their **limitations** and potential in terms of **scaling and transferability**, and by using these reflections to provide concrete recommendations, we offer food for thought for policy-makers, legal and law enforcement agencies, workplaces and the tech sector, as well as educators, practitioners and grassroots women's organisations.

1.2 Different forms of DGBV, between data and definitions

The terminology of DGBV.

Many online interactions can harm others and degenerate into abuse. Terms such as cyberviolence, online bullying, trolling, virtual violence and online hate crimes have entered the media discourse and are often interchangeably used[13]. While some of these (and others) may be appropriate in specific contexts and for given purposes, we **consciously use the**

---

person's sense of agency. As different individuals and groups, for very valid reasons, prefer referring to themselves by either term, we chose to use them both in our writing.

[11] Pew Research Center, 2014, op. cit.; Amnesty International Amnesty reveals alarming impact of online abuse against women, 2017, available at:
https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

[12] UN Human Rights Council, Resolutions on the "Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development", 2018, available at:
https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/_layouts/15/WopiFrame.aspx?sourced oc=/EN/HRBodies/HRC/RegularSessions/Session38/Documents/A_HRC_38_47_EN.docx&action=default&Defa ultItemOpen=1; OSCE, Survey on the Well-being and Safety of Women, 2019, available at:
https://www.osce.org/projects/survey-on-the-well-being-and-safety-of-women; European Parliament, Cyber violence and hate speech online against women, Study for the FEMM Committee, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union
PE 604.979 – September 2018.

[13] For a very thorough analysis of existing legal, academic and civil society actors' definitions, see European Parliament, 2018, op. cit.

concept of digital gender-based violence, and propose it as the most appropriate to be adopted by legislators, practitioners and advocates globally.

In fact, the concept of DGBV has the advantage of conveying that (1) we are looking at a violent phenomenon, whose **severe effects must be taken seriously**; (2) such violence is **motivated by gender** (which we define inclusively and keeping in mind how BAME, queer, poor, disabled, migrant women and people are more vulnerable to and less equipped to deal with abuse); (3) while DGBV takes place online, **its impact is extremely real**, and profoundly shapes the lives of individuals and communities.

Typologies of DGBV

For these reasons, we feel that juxtaposing 'virtual' or 'cyber' abuse to 'real life' abuse is unhelpful, and so are other definitions suggesting that online persecutions might represent less intense forms of harassment. On the other hand, we purposefully utilise the concept of DGBV as an **umbrella term encompassing multiple typologies of violent dealings**. Some of these constitute criminal offences in various countries, while others are covered by civil, international and EU legislation. Many of them overlap each other, and all are raising growing alarm among international women's and children's rights groups, digital safety experts and legal scholars. They include:

*Image-based abuse, also known as **non-consensual pornography** or revenge porn: online distribution of intimate photos or videos without the consent of the person appearing in the materials. The term **revenge porn**, rather popular with the mainstream media, alludes to the fact that perpetrators may have obtained the image in the course of a prior sexual relationship with the victims, and act in order to humiliate them as a form of retaliation. Yet **the term can be inaccurate and misleading**[14]. Graphic materials can be acquired without the knowledge of the victim or even a direct interaction with the perpetrator, for example by **hacking** the victim's computer, phone or accounts, or through **upskirting** (taking of surreptitious, sexually intrusive pictures, for example photographing underneath someone's clothes), or other forms of **digital voyeurism**. Equally, a survivor might have consented to the image being taken or shared with specific people, but not to its public distribution, or she might have been forced to share it or appear in it due to coercion or threat. At the same time, motivation for this act can go well-beyond personal revenge: they range from the perpetrator's **sexual gratification, to peer pressure and economic motives**. In fact, non-consensual pornography is fast turning into a genre that many (illegal) websites and providers specialise in[15], leading to disturbing forms of sexual exploitation and blackmail.

---

[14] See, for example, the discussion between IBA experts on the necessity to redefine revenge porn hosted by legal firm Bolt Burdon Kemp, available at: https://www.boltburdonkemp.co.uk/adult-abuse/revenge-porn-is-sexual-abuse/

[15] See Uhl, C. A., Rhyner, K. J., Terrance, C. A., and Lugo, N. R. 'An examination of nonconsensual pornography websites', Feminism & Psychology, 2018, 28(1), 50–68.

Statutory legislation on image-based abuse has been recently approved or is currently under review in various countries[16], and overlaps with **other criminal and civil offences** (rape, sexual harassment, threat, defamation and various types of privacy violations).

*Unsolicited pornography: sharing of sexually graphic materials without the consent of the recipient. This may stem from an ill-advised attempt to flirt, or a deliberate strategy to intimidate or humiliate the victim, ostracise her from a digital space or lure her into unwanted sexual activity. Regardless the intention, it can result into an equally triggering and traumatising experience for the receiver. **Vandalising** someone's social media and hacking their accounts to post or send explicit material may also fall into this category.

Other forms of (generally unlawful) **privacy-related online harassment** that may be determined by the target's gender include: **computer intrusion**, **doxing** (maliciously publicising online a person's private information, which often leads to an escalation towards offline violent episodes); **swatting** (electronically deceiving an emergency service into sending a response team to the victim's address); **impersonation** (stealing someone's identity to threaten them or discredit their reputation)[17].

*Cyber stalking: repeated harassment or intimidation via email, social media or other digital means. This practice may entail several of the actions discussed above, yet the **reiteration of the incident through time** is generally considered necessary to apply this specific category. As the repeated and persecutory nature of the act shutters the victim's **sense of safety** and causes fear, distress and other psychological damage, in many national legislations stalking behaviour (online and offline) constitutes **a criminal offence** (see Table 1). Importantly, online stalking often intersects with other abusive behaviours, such as **defamation**, **identity theft**, domestic and intimate partner violence and workplace harassment. It may also include attempts to gather information online that can feed into other violent actions.

*Gender-based online harassment and **ICT-related hate crimes:** regardless of the number and regularity of the incidents, hateful and gender-motivated attacks constitute a form of DGBV. This usually takes the form of aggressively **misogynistic** and highly **sexualised comments** shared via email, social media, forum or comment sections, or other messaging options. The comments may threaten **death and sexual or physical violence** (which constitute a crime in many countries), or be covered by national or international legislation on **hate speech and incitement to violence,** as well as defamation or bullying and sexual harassment at work. Furthermore, it is worth noticing that online hate campaigns are **often efficiently organised**, with the same victim (or collective) being simultaneously targeted by multiple perpetrators (which may include sexist, racist or homo-transphobic and other hate groups)[18].

---

[16] A comprehensive list of national provisions in this area can be found here: https://cis-india.org/internet-governance/files/revenge-porn-laws-across-the-world.

[17] For a comprehensive discussion, see Council of Europe, CyberCrime Convention Committee, Working Group on cyberbullying and other forms of online violence, especially against women and children. Mapping study on cyberviolence, 2018, available at: https://rm.coe.int/t-cy-2017-10- cbg-study/16808b72da

[18] Silva, L., Mondal, M., Correa, D., Benevenuto, F. and Weber, I., 'Analyzing the targets of hate in online social media', in Tenth International AAAI Conference on Web and Social Media, 2016.

*Digitally facilitated trafficking, sexual and economic exploitation: digital and electronic means can be used to facilitate the trafficking and exploitation of human beings, and –most evidently – the forced prostitution and involvement in pornography of women and children. In particular, ICTs serve to lure and coerce victims into **sexual and economic slavery**, allow traffickers, clients and other perpetrators to communicate and exchange money and information, and sustain the daily functioning of the trafficking industry. In particular, the term **digital grooming** specifically refers to fostering an online relationship with an underage person to pressure them into sexual activities, which can also include organised sexual exploitation[19]. On the other hand, digital technologies designed to harvest and monetise users' data can also facilitate the exploitation of women's bodies and work, by exposing them to **various forms of unpaid or underpaid labour and biopolitical control**[20].

DGBV figures

This non-exhaustive list encapsulates at least provisionally the existing millions of DGBV cases worldwide. Fresh data are still being collected and analysed by academic, public and third sector institutions, and more in-depth studies are needed to understand the specificities of different national contexts. Yet we already have **solid evidence** of the far reach and worrying extent of DGBV. The EU Agency for Fundamental Rights (FRA), for example, found that 20% of young women (18-29) in the EU have experienced online sexual harassment, and that 9 million European girls have undergone a form of digital gender-baseed violence by the time they were 15 years old[21]. According to the UN, women globally are 27 times more likely than men to be harassed online[22].

DGBV repercussions

Researchers have also started documenting the **effects** of DGBV. For instance, there are indications that the psychological consequences of experiencing cyberstalking are broadly **comparable with those of traditional stalking**, such as depressive symptoms, heightened anxiety levels, and posttraumatic stress responses[23]. More generally, costly consequences of various forms of DGBV include anxio-depressive disorders, as well as sleep disturbance,

---

[19] An exhaustive treatment of human trafficking falls out of scope of this policy paper. For further details see empadoo, K., Sanghera, J. and Pattanaik, B., Trafficking and prostitution reconsidered: New perspectives on migration, sex work, and human rights. Routledge: 2015.

[20] For a more thorough refection on the impact of digitalisation on biopolitics, labour, right to privacy as well as their gendered side, see, for example, Ajana, B. 'Digital health and the biopolitics of the Quantified Self', Digital Health, 2017; Fuchs, C., Capitalism, patriarchy, slavery, and racism in the age of digital capitalism and digital labour, Critical Sociology, 2018, 44(4-5), pp.677-702.

[21] EIGE, Cyber violence against women and girls, 2017, available online at: http://eige.europa.eu/rdc/eige-publications/cyber-violence- against-women-and-girls

[22] UN Broadband Commission for Digital Development, Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call, 2015, available online at: http://www.unwomen. org/-/media/headquarters/attachments/sections/library/ publications/2015/cyber_violence_gender%20report. pdf?vs=4259

[23] Worsley, J. D., Wheatcroft, J. M., Short, E., and Corcoran, R., Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses. SAGE Open: 2017.

and damages to women's **sexual and reproductive life**[24], together with **loss of self-esteem, confidence and concentration power**[25]. Existing studies from Europe, the US and Oceania[26] have also highlighted how victims of online violence might feel **deterred from using digital platforms**, or (this is especially the case for female journalists, politicians and activists) may find that their professional performances suffered significantly and **consider abandoning their jobs** and commitments. Furthermore, cases of attempted suicide and post-traumatic stress disorder are particularly common among survivors of DGBV[27]. Finally, whilst repercussions of digitally facilitated trafficking and other forms of sexual and economic exploitation deserve a separate analysis, we refer to the literature cited in the above footnotes for a thorough examination of their profound impact.

Building on these conceptual tools and data, our paper aims to showcase and analyse good practices that counteract DGBV in its different forms and attempt to tackle its manifold implications. We recognise that terminology and research strategies are not politically neutral, and have made definitional and research design choices that reflect our main goal: improving public understanding of DGBV, and helping relevant stakeholders address it effectively.

A note on methodology

The case studies and recommendations in this report are based on the examination of existing practices of resistance against DGBV. Our investigation process included both desk research and the gathering of empirical data through semi-structured interviews with experts and practitioners, as well as primary source document analysis and observations collected in various contexts.

As in our previous works, we have been inspired by the principles of Action Research (AR)[28], an approach that aims to identify shared solutions to pressing social problems through the use of participatory and interactive methods for data collection and analysis. AR key components are:

---

[24] Muriel Salmona cited in Haut Conseil à l'Egalité, En finir avec l'impunite des violences faites aux femmes en ligne : une urgence pour les victimes, 2017, available at http://www.haut-conseil-egalite.gouv.fr/IMG/pdf/hce_rapport_violences_faites_aux_femmes_en_ligne_2018_02_ 07.pdf
[25] Amnesty International, Amnesty reveals alarming impact of online abuse against women, 2017, available at: https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals- alarming-impact-of-online-abuse-against-women/
[26] UNESCO, Building Digital Safety for Journalists, 2015, available at: https://ipi.media/online-abuse-of-journalists-has-deep-psychological-impact-experts-say; Amnesty International, 2017, op. cit., Atalanta, (Anti)Social Media. The benefits and pitfalls of digital for female politicians, 2018, available at: https://www.atalanta.co/news/2018/3/13/antisocial-media-the-benefits-and-pitfalls-of-digital-for-female-politicians;
[27] See Wood, L, Voth Schrag, R. and Busch-Armendariz, N. 'Mental health and academic impacts of intimate partner violence among IHE-attending women', Journal of American College Health, 2018;
Kamal, M. and Newman, W.J., 'Revenge Pornography: Mental Health Implications and Related Legislation', Journal of American Academy of Psychiatry Law, 2016 Sep;44(3):359-67; see also UNICEF FRANCE, Ecoutons ce que les enfants ont à nous dire, Consultation nationale, 2014 available at: https://www.unicef.fr/sites/default/files/userfiles/Consultation_2014.pdf
[28] See Reid, C. J., 'Advancing women's social justice agendas: A feminist action research framework', in International Journal of Qualitative Methods, 2014: 3(3). Article 1.

- 'Knowing comes from doing': researchers are expected to work closely with practitioners (or to be practitioners themselves).
- Partnership and participation: the purpose of AR is emancipatory (i.e. empowering real people and communities to solve real-life problems).
- Actionability: AR should provide relevant stakeholders with tools and solutions that fit their contexts. Therefore, researchers are supposed to let emerge research participants' actual needs, collaborate with them to pinpoint suitable points for actions, and disseminate their studies through appropriate and widely accessible channels.

1.3 Complex ramifications call for multi-level solutions

Old violence

Like any forms of gender-based abuse, DGBV has complex causes that reside in **centuries of patriarchal norms and structures**. While important progress has been made, die-hard sexist **stereotypes still shape modern visions of power, labour distribution, sexuality, family and spirituality**. Women are attacked, abused and exploited online as their gender, and often their ethnic, religious, class background, sexual orientation or disabilities[29], are perceived as a **threat to the oppressive status quo[30]**. As they voice their opinions online, use technology to reshape their working and personal lives or take political action (writing, defending social causes, running for office, intervening in public debates), or by simply accessing the Internet to enjoy themselves, women challenge an entrenched system of repression. In its multiple forms, DGBV reflects the attempt to deprive half of the world's population of that freedom, exclude them from increasingly digitalised economic, political and cultural arenas, while exploiting and subjugating their bodies, sexuality and labour.

Furthermore, **the tech industry mirrors historical patterns of gender inequality**. As a consequence, recent research shows[31] that decision-making processes often overlook the intersections between gender and digitalisation, and gender bias is incorporated in the coding of algorithms and AI-based solutions. As courageously pointed out by many women in the

---

[29] The online abuse of disabled women is among the most understudied aspects of DGBV. For a more thorough examination of the phenomenon, see, for example, UK Parliament, 'Online abuse and the experience of disabled people', last accessed November 2019, available online at:
https://publications.parliament.uk/pa/cm201719/cmselect/cmpetitions/759/75905.htm.

[30] See Jane, E.A., "Back to the kitchen, cunt": speaking the unspeakable about online misogyny', Continuum: Journal of Media & Cultural Studies, 2014, Vol. 28, No. 4, 558–570.

[31] See Brey, P., 'The Technological Construction of Social Power', in Social Epistemology 22, 71–95, 2007; Dastin, J. Amazon scraps secret AI recruiting tool that showed bias against women, last viewed 20 December 2018, accessible at: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G; Noble, S. Algorithms of Oppression. New York: NYU University Press: 2018.

tech sector[32], a sexist culture is also rife within the digital space, including countercultural, **non-mainstream digital coteries** that are often presented as social innovation hubs and fertile grounds for social justice movements.

Novel tools

At the same time, the very nature of the digital space produces some phenomena that are specific to DGBV. The Internet is still largely unregulated and **shaped by a few powerful actors**, and many platforms grant **anonymity and substantial impunity** to their users, including violent and exploitative ones. Social media and other forms of online communication, while empowering activists to coordinate, also allow DGBV perpetrators to work together and **act simultaneously** against their victims, often from across different countries and time zones. In cases of image-based abuse, online stalking and gender-based hate speech, organised attacks can also effectively **isolate the victim**, whose accounts are invaded by abusive slurs and offensive materials, making it harder for her to reach out for help[33]. Similarly, as ICTs have become an important component of professional and personal life, instances of DGBV may reach the victim in the perceived safety of their homes or in their workplaces[34]. This shatters their sense of safety, while **the eco-chamber effect** typical of social media platforms may enhance their sentiment of isolation, loneliness and powerlessness. Finally, the difficulty of permanently removing abusive or triggering content from the Internet, which obliges the survivor to re-experience their victimisation all over again, is also an unprecedented characteristic of DGBV.

Solutions on the table

Due to these complexities and pervasive ramifications, it is clear that **tackling DGBV requires a multi-level approach**, and that solutions must involve not only lawmakers and digital safety professionals, but also educational and cultural institutions, health providers, workplaces, grassroots groups, and -crucially- the tech industry.

In the last few years, in fact, international human rights organisations have intensified their effort to map DGBV instances, and to identify good practices locally, nationally, and transnationally. Suggestions have so far included **developing a statutory, international definition** of digital violence against women, and translating this into new or reinforced **national provisions**[35]. It has also been emphasised that effective **reporting and intervention mechanisms** should be created, and **funding** devolved to supporting survivors. Furthermore,

---

[32] See Faulkner, W. and Lie, M., 'Gender in the Information Society: Strategies of Inclusion', Gender, Technology and Development 11, 157–177, 2018; Lohan, M. and Faulkner, W., 'Masculinities and Technologies: Some Introductory Remarks', Men and Masculinities 6, 319–329, 2001.

[33] See Phillips, J., Every woman, One woman's truth about speaking the truth, Penguin Books: 2017, for a first-person account of this phenomenon.

[34] See Penny, L., Cyber sexism, A&C Black: 2013, available online at: https://fleurmach.files.wordpress.com/2017/07/laurie-penny-cybersexism-sex-gender-and-power-on-t.pdf; Mantilla, K., Gendertrolling; how misogyny went viral, ABC Clio: 2015.

[35] UN Broadband Commission for Digital Development, 2015, op. cit.; FRA, 2017, op. cit.; European Parliament, 2018, op. cit., EWL, #HerNetHerRights. Resource Pack on ending online violence against women & girls in Europe, 2017, available online at: https://www.womenlobby.org/IMG/pdf/hernetherrights_resource_pack_2017_web_version.pdf

due to the novel character of DGBV, it has been proposed that law enforcement personnel should be adequately **trained** to recognise and deal with criminal online behaviours. Some groups have further argued that tech companies and **social media platforms should be made responsible for the content** they share, and pushed to adopt more effective reporting and take down procedures, as well as to take sexism, women's and human rights more seriously[36].

The **debate on policy reform** and **tech sector regulation**, however, is complicated by the differences between legal systems and cultures. In Anglo-American countries, for example, concerns related to free speech are often juxtaposed to attempts to strengthen legislation on hate speech[37]. National provisions on hate crimes, defamation, sexual violence as well as data treatment and privacy may also differ substantially from a legal context to another.

At the same time, the importance of **prevention work**, and **educational interventions** in particular, have been often underlined. It has been rightfully emphasised that not only young people, but Internet users of all ages should be educated to become responsible digital citizens. With this in mind, experts and advocates have called for **further data collection** and specialised studies of DGBV, as well as for **awareness-raising campaigns** to inform about the phenomenon, empower women to resist it, and help **shift the media conversation** on digitalisation.

Yet educational reforms in this area are a highly politicised topic, too: **opposition** to the introduction of gender-related concerns into sexuality and education programmes is growing stronger in many Western countries. Similarly, the **space accorded to civil society**, and especially feminist organizations, is shrinking globally, as their work is attacked by conservative media and politicians, and their opportunities to gain funding and institutional support have notably shrunk[38]. To put it differently, experts' and activists' comprehensive **recommendations need now to be tested and refined** through the analysis of real-life case studies, to help overcome these obstacles and enhance and scale existing progress. We have thus selected for analysis and discussion **six examples of such practices**, which we briefly summarise here below.

How and why our selected cases can help

In our first case, scrutinising Australia's recent legislation on **image-based abuse**, we examine how **new laws** can successfully contribute to prevent and sanction a particularly invasive form of DGBV, which existing legal instruments were not able to capture. We also consider the advantages of particular legal definitions and understandings, and the limits of standalone policy reform.

In our second case, we investigate how a transnational women's organisation, European Women's Lobby (EWL), partnered with Google on a DGBV-related project. We treat this as a

---

[36] See, for instance, APC Women's Rights Programme, Technology-related Violence Against Women, Briefing paper on VAW, June 2015.

[37] For an exhaustive discussion, see Citron, M., Hate Crimes in Cyberspace, Harvard University Press: 2014.

[38] Kvinna Foundation, Suffocating the movement – Shrinking space for women's rights, 2018, available online at: https://kvinnatillkvinna.org/2018/10/05/suffocating-the-movement/

case of **cross-sector partnership**, analysing from EWL's perspective the benefits of the collaboration. While focusing on lessons to be learned for other **research and advocacy initiatives** aimed at mainstreaming feminist and social justice concerns into the tech industry, we also reflect on the risks entailed in this kind of cooperation.

Our third and fourth cases, both from the United Kingdom, provide us with insights into the complementary benefits and drawbacks of two opposite strategies for **awareness raising, training and educational efforts**. On the one hand, we look at Childnet, an **established charity** from the field of digital safety and children's rights, which developed **gender-sensitive projects** and used its existing resources and social capital to bring DGBV to the attention of its beneficiaries and target audiences. On the other hand, we illustrate the trajectory of **Glitch!**, a **single issue advocacy organisation** specifically created to educate the public and lobby policy makers and tech companies on DGBV and racist online abuse.

We then focus on a case **survivor-centred in-depth reporting** from Romania, which blended academic research, journalistic investigation, grassroots educational work, as well as political lobbying surrounding DGBV issues. The story is told in first person by the leading reporter, who incorporates elements of retrospective analysis, and is accompanied by a few considerations from the GenPol team.

Finally, we examined **the most interesting software-based solutions** in the field of online content moderation and DGBV reporting mechanisms. In so doing, we take into consideration both the impact of different moderation policies on tech company employees, and the risk that AI instruments may concur to perpetuate existing gender biases.

All case studies shed light on the reality of implementing policy recommendations and anti-DGBV solutions. Based on this, we offer some updated, thorough recommendations for different stakeholders in the past part of this paper.

Table 1

Examples of national legislation on online stalking

Country	Legislation	Details
UK	Protection from Harassment Act 1997 Protection of Freedoms Act 2012 https://www.cps.gov.uk/legal-guidance/stalking-and-harassment	Covers cyber stalking.
New Zealand	Harmful Digital Communications Bill 2015 https://www.loc.gov/law/foreign-news/article/new-zealand-legislation-aimed-at-preventing-and-punishing-cyberbullying-passed/	The legislation, which was originally introduced in November 2013, establishes complaint mechanisms for victims of behaviour such as cyberbullying, harassment, and "revenge porn" and will provide new civil remedies and criminal offenses.
Queensland, Australia	Stalking Amendment Act 1999 https://www.haltabuse.org/resources/laws/australia.shtml	Includes use of any form of technology to harass a target as forms of "criminal stalking".
California, United States	California Stalking Laws Penal Code https://www.shouselaw.com/cyberstalking.html	"Cyberstalking" was officially prohibited in 1998 when the California Legislature amended Penal Code 646.9 stalking. The amendment changed the definition of "credible threat" (one of the elements of the crime of stalking in California)..to include "electronically communicated" threats.

Poland	Polish Criminal Code 2011 https://eige.europa.eu/gender-based-violence/regulatory-and-legal-framework/legal-definitions-in-the-eu/poland-stalking	Cyberstalking becomes illegal.

Part 2

Good practices and lessons to be learned

The case for policy reform: Australian legislation on image-based abuse

By Nathalie Greenfield

The problem: growing rates of image-based abuse. In May 2017, a hard-hitting report by researchers at RMIT University unveiled the scope and effects of digital violence in Australia. The authors found that one in five Australians had experienced image-based abuse (IBA). Such abuse included having images taken or distributed without the victim's consent, or receiving threats to this effect[39]. The report unearthed the **gendered nature** of IBA and the need for an **intersectional analysis** of the phenomenon. In fact, whilst women and men were equally likely to report being a victim of IBA, only 33% of perpetrators appeared to be women, and women were also more likely to fear for their safety due to digital violence[40]. Furthermore, researchers found that marginalised groups were especially vulnerable to IBA, as is the case with many forms of gender-based abuse. Specifically, half of surveyed Australians who identified as either Indigenous or disabled reported surviving IBA, and rates of victimisation also increased within the LGBTQ+ community. Perhaps unsurprisingly, the research indicated those aged 16 to 29 as at a higher risk of experiencing IBA[41].

The (legal) context. In response to the preponderance of DGBV and IBA, Australian policy-makers have begun to tackle IBA through **legal means**. Of Australia's six states and two territories, five states have adopted legislation regarding image-based abuse. The first IBA legislation in the country was passed in 2014 in Victoria, and public demand has since fuelled academic studies, political inquiries, and legislative change across the entire nation. As of 2019, only three jurisdictions (Queensland, Tasmania, and the Northern Territory) remain without statutory laws in this area[42].

It is worth noting that there is **currently no nationwide criminal statute** addressing digital abuse. Rather, the Australian government has been exploring the possibilities presented by **civil, as opposed to criminal, penalties[43]**. Specifically, in November 2015, the Australian Senate referred the issue of revenge porn to the Senate Legal and Constitutional Affairs References Committee for inquiry. In 2016, the Committee produced a report that recommended considering civil law penalties, including take-down notices, as a chief measure to combat the growing incidence of so-called revenge porn[44]. The executive responded in

---

[39] See Henry, N., Powell, A., and Flynn, A., Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse, Melbourne: RMIT University, 2017, available online at:
https://research.monash.edu/en/publications/not-just-revenge-pornography-australians-experiences-of-image-bas, p. 4, 5. This researched surveyed 4,274 participants.

[40] Ibid., p. 5-7. (54% of perpetrators are male, according to the report, while 13% are 'unknown'.)

[41] Ibid., p. 5-7.

[42] For further information on existing Australian legislation in this area, see: ACT, Crimes Act 1900 § 72; NSW, Crimes Act 1900 § 91Q; SA, Summary Offences Act 1953 § 26B-C; VIC, Summary Offences Act 1966 § 41DA; WA, Restraining Orders and Related Legislation Amendment (Family Violence) Act 2016, § 10G/61.

[43] In common law jurisdictions like the UK, the USA, and Australia, civil law affords different remedies to criminal law. Civil law awards damages (such as monetary remedies) and affords injunctive relief (i.e. a court order to refrain from an act), whereas criminal law results in a conviction and punishes and individual.

[44] Australian Government, 'Civil penalties regime for non-consensual sharing of intimate images: Discussion paper', Canberra: Commonwealth of Australia, 2017, p.7. The Committee also recommended measures such as adopting criminal law penalties, public education and awareness campaigns, and police training.

May 2017, by proposing a civil penalties regime for IBA, and suggesting specific measures such as issuing injunctions, infringement notices, take down notices and formal warnings.

Since then, the Australian legislative framework for responding to IBA and digital abuse has been fast-developing. In order to illuminate the strengths and possible drawbacks of the Australian case and of legal solutions to DGBV more generally, it is helpful to focus specifically on **legislative change in one Australian territory: New South Wales.**

Good practice: The Crimes Amendment (Intimate Images) Act in New South Wales. Until 2017, there were some successful attempts to use existing New South Wales legislation to prosecute revenge porn. For example, in 2011 the territory prosecuted a man who had posted intimate photos of his ex-girlfriend on Facebook under § 578 of the Crimes Act 1900 and sentenced him to six-months imprisonment[45].

In 2017, however, New South Wales **passed legislation which created three new offences** under the Crimes Act 1900[46]. Sections 91P and 91Q of the Crimes Act 1900 now make it a crime to **intentionally record** and **intentionally distribute** an intimate image of another person without their consent. Both of these offences carry a maximum penalty of 3 years imprisonment[47]. Similarly, § 91R extends this provision to those who **threaten to record or distribute** intimate images without the permission of the interested person. Such a threat can be made by conduct, can be explicit or implicit, can be conditional or unconditional, and can be made irrespective of whether the image actually exists[48].

Furthermore, the Act's definition of "intimate image" is extensive: it refers to any images of a person engaged in a private act, such as being undressed, using the toilet, shower or bath, engaging in a sexual activity, as well as images of a person's breasts, genital or anal area, whether bare or covered by underwear. Importantly, the new legislation stipulates that if a court finds a person guilty of a § 91P or § 91Q offence, the court can order the removal, retraction, deletion, or destruction of the image, or take other reasonable actions. At the same time, a person under the age of 16 cannot be prosecuted for an IBA offence without the approval of the Director of Public Prosecutions.

Strengths and shortcomings: does the law match the problem? New South Wales' legislation on IBA is **comprehensive**. It covers acts as well as threats, treats minors differently to adults, and contains punitive and injunctive penalties. Moreover, it has **already seen use**. For example, in September 2017 a 20-year-old man was charged under the Act's IBA provisions for extracting intimate images from a 14-year-old girl and threatening to circulate the images unless she had sex with him[49]. His actions **would not have been sanctionable under previous law**, which suggests that the legislative reform is targeting exactly the kind of digital abuse it was designed to prevent.

---

[45] Police v. Ravshan Usmanov, 2011, NSWLC 40, see
<https://www.caselaw.nsw.gov.au/decision/54a636e73004de94513d973b>
[46] NSW, Crimes Amendment (Intimate Images) Act, <https://legislation.nsw.gov.au/#/view/act/2017/29/full>
[47] NSW, Crimes Act 1900, available online at:
<https://www.legislation.nsw.gov.au/#/view/act/1900/40/part3/div15c/sec91p>; definitions of 'intimate' and 'consent' are provided in § 91N. Importantly, being reckless as to whether the person consented to the recording is prosecuted with the same severity, as is knowing that the person did not consent to the recording.
[48] Ibid., § 91R
[49] Tonkin, S., 'Police officer's son among first to be charged in NSW over 'revenge porn'', Sydney Morning Herald, 29/09/2017 <https://www.smh.com.au/national/nsw/police-officers-son-among-the-first-people-charged-in-nsw-over-revenge-porn-20170929-gyr1gd.html>

Moreover, the new legislation responds to the most common forms of abuse outlined by academic and policy research. It **does not limit its scope to domestic relationships** (as is unfortunately the case in Western Australia). Equally importantly, the **perpetrator's motivation is irrelevant** under the new law, which closes a previous legal loophole whereby a person could have escaped prosecution if the images had not been taken for sexual gratification. Here, the focus has rightfully shifted to victims and survivors, to the wrong done to them, and the harm they have suffered.

Whilst Western Australia Shadow Attorney-General Michael Mischin has observed that this may allow for "stupidity, naivety and immaturity rather than criminality" to be a basis for prosecution, it is worth emphasising that whether images are shared by a naïve ex-partner or a professional porn producer does not mitigate the harm to the victim[50]. Making actions, and not motivation, the basis for culpability in IBA thus appears appropriate.

Another important strength of this legislation is its differentiation between adults and children under 17. The purpose of the law is not to criminalise sexual activity between young people but rather to target predatory and harmful conduct. To this end, the law rightfully differentiates between age groups, with the caveat that the state can nevertheless pursue prosecution of a minor should it deem this appropriate[51]. In other words, juvenile IBA emerges as a domain in which education, and not over-criminalisation, should step in, so as to facilitate the **healthy development of youth sexuality.**

Several **concerns**, however, remain. First, the law enables judges to order the removal of online intimate images, yet it is hard to see how this can truly be possible in the digital age. Once data has been uploaded to a social media, chat, or porn site, the web of its shares and downloads can quickly become a labyrinth that makes **removing an image's trace from the Internet** a quasi-impossible task. Moreover, Australian courts do not have jurisdiction to issue take-down orders over websites which lack a sufficient connection to Australia. Indeed, IBA is a **global problem**[52]**, which requires inter-state cooperation.** States must push for tech giants and foreign governments to collaborate with national authorities.

Another aspect that deserves further attention is the gendered nature of IBA, and the specific vulnerability of marginalised people and communities. More firmly placing IBA in the domain of sex crimes (a categorisation already identified by the Australian E-Safety Commissioner[53]) would help **reinforce the association between IBA and other forms of gender-based violence**. To effectively implement the new law, law enforcement personnel must be made aware of how online and offline violence motivated by gender intersect, and of the ways in which patriarchal power dynamics play out between IBA perpetrators and victims. Similarly, overwhelmingly high rates of abuse amongst disabled or Indigenous Australians should be

---

[50] Goldsworthy, T., 'Revenge porn laws may not be capturing the right people', The Conversation, 28/09/2017, <https://theconversation.com/revenge-porn-laws-may-not-be-capturing-the-right-people-84061>

[51] See also Frayne, A., ''Three years' jail for revenge porn under new laws in NSW', Stacks Law Firm: News, 02/08/2017 <https://www.stacklaw.com.au/news/criminal-law/three-years-jail-revenge-porn-new-laws-nsw/>

[52] See The Economist, 'Misery Merchants', The Economist 05/07/2014, <https://www.economist.com/international/2014/07/05/misery-merchants>

[53] Australian Government, Submission on the 'Phenomenon colloquially referred to as 'revenge porn', Canberra: Commonwealth of Australia: 2016, p.2: "The non-consensual sharing of private sexual images can be a form of family violence or sexual abuse."

tackled through **police and prosecutor training**, as well as targeted public awareness campaigns.

Lessons to be learned. There is much that other countries can learn from New South Wales' IBA legislation. New South Wales' criminal provisions are an important foundation, and provide a clear line as to what a society will not tolerate. However, if the law cannot address specific harms to marginalised groups, then it becomes less effective. Forward thinking legislatures must drive forward educational and social programmes, and legislation must be introduced in tandem with other measures, such as legal staff training, social awareness initiatives and the devolvement of funds to support survivors. Further, exploring civil remedies alongside criminal penalties, as the Australian government is doing at federal level, is another important tool that can inform a multifaceted approach to tackling DGBV.

Finally, IBA requires the creation of a specifically-targeted criminal offence in most legal systems, due to the specific characteristics of the phenomenon and the legal loopholes it has created in many countries. However, **creating new offences must not be done lightly**. It is critical that police and prosecutor training is implemented to ensure that laws do not over-criminalise, that victims receive adequate support, and that the law acts as a deterrent. The ultimate goal, after all, must be the prevention of IBA and all forms of gender-based abuse.

Raising awareness within the tech industry: European Women's Lobby Partnership with Google

By Mariana Plaza, Ciara Taylor & Lilia Giugni

The context and the problem: raising awareness of DGBV at the EU level. European Women's Lobby (EWL) is the largest umbrella organisation of women's organisations in the European Union. Based in Brussels, it represents more than 2000 women's civil society organisations and has worked since 1990 to promote women's human rights and influence European institutions in favour of equality between women and men[54]. Ending violence against women in Europe has long been one of EWL's priorities[55]. This has led, among other actions, to the creation in 1997 of a specific Observatory[56], as well as to multiple EU- and country-level initiatives towards the ratification of the Istanbul Convention.

Since 2015-16, EWL recognised the escalation in digital violence against women and girls as a burning issue, concluding that Internet-based technologies had both reinforced existing forms of gender-based abuse and created new violent practices. Having identified DGBV as a key area of work, the organisation set itself a threefold task. First, it aimed to **create awareness across EU institutions and other relevant stakeholders on the gendered nature of digital abuse**, presenting it as **a part of the continuum of violence against women and girls**, whose impact needs to be taken as seriously as those of physical and sexual attacks. Second, due to the scarcity of credible research in the field, EWL intended to **map the state of DGBV** and the specific forms that it takes in EU Member States, together with its political, social and economic implications. Building on this, appropriate **policy recommendations** were to be put forward with the purpose of building a safer and more gender-equal Internet. Third, EWL was determined to adopt **a survivor-centred approach**, providing a platform for the stories, needs and suggestions of those who survived DGBV, and paying a special attention to intersecting vulnerabilities.

In 2017, these efforts translated into the launch of the **#HerNetHerRights project**, which combined two distinct sets of activities. The first part included the drafting of a **mapping report**, and culminated in the launch of a **resource pack** and an **online conference** in 2017. The second part (#HerNetHerRights2) saw the implementation of an intersectional **training on online violence specifically tailored around women politicians** as part of a wider effort coinciding with the European Elections campaign. This was meant to create resources for EWL member organizations to conduct trainings sessions at national level in 2018-19[57]. Interacting, lobbying on, and potentially cooperating with **the tech industry** was essential for these activities, and we chose to examine the steps and outcomes of the solution that EWL adopted. Examining the case from EWL's perspective, we draw insights on the effectiveness, challenges

---

[54] See Helfferich, B. and Kolb, F., Multilevel action coordination in European contentious politics: the case of the European Women's Lobby, Contentious Europeans: protest and politics in an emerging polity, 2001, pp.143-161.

[55] https://womenlobby.org/25-years-of-European-Women-s-Lobby?lang=en

[56] See https://womenlobby.org/List-of-experts?lang=en

[57] See #HerNetHerRights. Resource Pack on ending online violence against women & girls in Europe, available online at: https://www.womenlobby.org/IMG/pdf/hernetherrights_resource_pack_2017_web_version.pdf

and benefits of **cross-sector partnerships**, and of the involvement of tech actors in DGBV-related initiatives.

***Good practice: the partnership between European Women's Lobby and Google**. Building on the above-mentioned evaluations, EWL's Programme Hub was approached by Google as a potential partner and interlocutor, and started fostering contacts with the company's team in Brussels. The primary liaison between the two organisations was Sara Elnusairi, Global Public Affairs Senior Manager at Google in Brussels. Having a thorough understanding of Google's relations with the civil society as well as a background in EU public policy, Elnusairi was able to serve as an effective entryway, providing useful inputs and agreeing with EWL on mutually beneficial goals. Moving forward, another contact-point for EWL was the team at Jigsaw, an Alphabet arm focused on cybersecurity and geopolitical issues, including the use of artificial intelligence to pinpoint cases of online violence[58].

These positive first contacts, according to EWL's members of staff[59], helped create expectations that the **partnership would benefit everyone involved[60]**. On the one hand, EWL obtained financial support for the #HerNetHerRights project from Google, as well as valuable insights regarding tech-based solutions to DGBV. On the other hand, Google recognised the expertise of EWL in the area, the importance of the ethical and political concerns that they raised, and the reputational advantages that stemmed from the cooperation. This ensured an **active engagement** and constantly good communication on both parts.

The partnership has so far led to several significant results. First, by **funding EWL's research and advocacy efforts**, Google has concurred to support the production and distribution of findings on the extent of DGBV in Europe, summarised in a few **publications**[61] and made public through several events (including the above-mentioned **e-conference,**[62] which brought together experts, activists, survivors and other relevant stakeholders). Among the most important conclusions of the project were findings surrounding the fact that violence against women is largely neglected in the internal regulation of online spaces (especially in comparison to cases of homophobic or racist speech), and that anonymity and the lack of repercussions are amid the main factors encouraging perpetrators of DGBV.

Second, the partnership with Google has provided EWL with **further support and an extended platform** for their DGBV-related initiatives. In the second part of the project (2018-2019), EWL developed, as we saw, a training programme for European female politicians, including digital self-care strategies and tools that women running for office may use to deal with online attacks, together with policy recommendations to tackle the issue at legislative level. Well-received training modules also drawing on the partnership with Google have already taken

---

[58] However, details on the controversy that surround Jingsaw's own internal culture and its sexist traits can be found here: https://www.businessinsider.com/jigsaw-toxic-culture-raises-concerns-2019-7?r=US&IR=T.

[59] Our analysis of this specific good practice draws on interviews with EWL staff, as well as an examination of the outputs produced during the collaboration.

[60] See Le Ber, M.J. and Branzei, O., (Re) forming strategic cross-sector partnerships: Relational processes of social innovation, Business & Society, 2010, 49(1), pp.140-172.

[61] See https://www.womenlobby.org/IMG/pdf/hernetherrights_resource_pack_2017_web_version.pdf and

[62] https://www.womenlobby.org/Watch-HerNetHerRights-online-conference-here and https://www.womenlobby.org/IMG/pdf/facsheet_violence_against_women_and_girls_in_europe_2017_website.pdf

place in six Member States, involving over 300 politically engaged women and 102 MEP candidates for the May 2019 elections, and at various European Institutions. EWL is currently evaluating how to develop this tool further for their membership to continue disseminating findings and good practices at national level. Additionally, EWL seeks to adapt this programme to other demographics, including young women and women human rights defenders, and on particular issues such as pornography and trafficking. Building on this work, the organisation is also campaigning for legislative frameworks on violence against women capable to capture DGBV cases, and for an increase in prosecutions of online abuse-related crimes.

Strengths and potential drawbacks of cross-sector partnerships. The successful history of #HerNetHerRights shows that cross-sector partnerships can be a valuable instrument to address multi-faceted problems, and that it is crucial to get tech companies involved in the fight against DGBV. As highlighted by Asha Allen, Policy and Campaign Officer at EWL and a DGBV expert, the positive impact of their collaboration with Google is reflected in the **partners' mutual interest in cooperating during the 2019 European Election campaign and the fact that DGBV, as framed during their common project, is now high on the European political agenda.** Overall, EWL felt that the cooperation contributed to develop a more thorough understanding of the **evolution of gender-based abuse in modern times**, as well as to brainstorm and exchange good practices between all key players. Furthermore, closely working with Google has been a significant contribution to EWL's **penetrating the space of global tech industries,** that remains unrepresentative of the diversity of the digital space, and to start mainstreaming intersectional feminist themes in that industry.

That being said, throughout the entire project, the **key priority for EWL has been to remain a prominent voice on DGBV** and ensure that feminist concerns gain visibility within the debate on digital innovation and online safety. **Large tech companies**, including the most collaborative ones, **continue to be a crucial part of the problem**. There is evidence that more could be done in terms of allowing access to data on DGBV, introducing more effective internal regulation and moderation settings, and timely supporting survivors. Further, the **sexist culture** that characterises a substantial part of the digital industry, as well as **the ways in which digitalisation has reinforced patterns of discrimination and exploitation of women** and various vulnerable categories, still remain to be addressed. EWL, like any women's rights group, is forced to **navigate relationships with tech actors while being aware of these complexities**, and in the knowledge that private companies must be constantly pushed to engage in concrete actions that go beyond good intentions and PR exercises[63]. With this in mind, EWL generally conducts comprehensive consultative procedures, due diligence and risk analysis with members prior to engaging potential funders.

Lessons to be learned. The cooperation between EWL and Google provides a **high-level, promising example** for actors from individual EU Members States (and non-EU countries) to draw inspiration from. The scope of the partnership was relatively broad, extending to research collaboration, financial and logistical support provided by Google for EWL's initiatives, and mutual exchanges of inputs on creative solutions. Importantly, through specially designed training, mutually built collaborative practices, and regular interactions at

---

[63] See, for example, Lubitow, A. and Davis, M., 'Pastel injustice: The corporate use of pinkwashing for profit', Environmental Justice, 2011, 4(2), pp.139-144.

senior management level, EWL also felt enabled to **push feminist insights more deeply** into Google's organisational life.

Naturally, not all national – or grassroots-based – women's rights groups[64] possess the resources and social capital which make EWL a valuable interlocutor for a leading tech company. Similarly, other digital platforms (especially in the social media space, where cases of online abuse are particularly significant) are less open than Google to start productive conversations on regulation, and on **platforms' responsibility for digitally shared content**. It is also worth noting that a critical dimension of the collaboration between EWL and the Google office in Brussels lay in geographical proximity and in the **personal character of their relationship.** This latter aspect indicates that **finding knowledgeable and passionate gatekeepers from the private sector** might be particularly helpful in framing and keeping mutually beneficial connections – a strategy that could be borrowed by various gender equality advocates.

A final, central lesson that might be learned from this case concerns precisely the multifaceted **scope of the collaboration** itself. In fact, while working together to produce specific findings and outputs, the two partners **created a space for other meaningful interactions** to happen in the form of training of the EWL Women in Politics Working group and Observatory on violence against women. This allowed them to achieve positive results, whilst maintaining their respective roles and different missions.

---

[64] See Silliman, J., Expanding civil society: Shrinking political spaces—The case of women's nongovernmental organizations, Social Politics: International Studies in Gender, State & Society, 1999, 6(1), pp.23-53; Clark, C., Sprenger, E., VeneKlasen, L., Durán, L.A. and Kerr, J., Where is the money for women's rights? Assessing resources and the role of donors in the promotion of women's rights and the support of women's organisations, 2006.

Mainstreaming intersectional feminism within an existing charity: the case of Childnet

By Ciara Taylor & Lilia Giugni

The problem and the context: how to use existing resources to address a new problem?
Childnet International is a non-profit organisation aiming to make the Internet an enjoyable and safe place for children. Since 1995, they have worked directly with young people aged 3-18, as well as parents, carers, teachers and professionals, collecting data about young people's experiences online and suggesting solutions to enhance digital safety. This includes the awareness-raising initiative Safer Internet Day, and campaigns against various forms of online abuse[65].

While Childnet's primary beneficiaries are **children** of all genders, their approach to project management reveals that they have gradually and effectively **integrated an intersectional feminist perspective** into their line of work. In particular, due to the passion and interest of some members of their executive team, Childnet's Policy and Communications Manager Maithreyi Rajeshkumar and Education and Youth Engagement Manager Ellie Proffitt, gender- and race-related concerns have been constantly mainstreamed into one of the organisation's leading projects, deSHAME[66]. Born as a collaboration between Childnet, Save the Children (Denmark), Kek Vonal (Hungary) and UCLan (UK), and co-financed by the EU, this research programme provided a space for the organisation to raise awareness of the gendered traits of peer-based online harassment. We examined this work as an example of **feminist intrapreneurship[67]**, i.e. a case in which employees of an established organisation were able to make the most of their organisational context and resources to help address a gender-related problem.

Good practice: Project deSHAME. The project[68] focuses on researching young people's experiences of online sexual harassment, and specifically emphasises the gendered characteristics of the phenomenon and its intersections with other forms of violence against girls and non-binary youth. Methods used for the final report included surveys, focus groups and interviews with young people, teachers and other professionals.

The project's **research findings[69]** revealed that the majority of the children involved did learn about online sexual harassment at school, but did not find what they learned particularly helpful. It was also found that young people are less likely to report a case of online sexual harassment to a social media network, the police, a helpline or teachers, than they are to speak to friends or family. Importantly, researchers concluded that digital harassment takes place in

---

[65] https://www.childnet.com/what-we-do
[66] https://www.childnet.com/our-projects/project-deshame
[67] See Tracey, P. and Stott, N., 'Social innovation: a window on alternative ways of organizing and innovating', Innovation, 19(1), 2017, pp.51-60.
[68] Our analysis draws on interviews with Maithreyi Rajeshkumar and Ellie Proffitt from Childnet, as well as the examination of the project's outputs.
[69] Report available at https://www.childnet.com/our-projects/project-deshame/research

a gendered context, and produces disproportionately negative outcomes and experiences for girls. Researchers also underlined how sexual harassment can intersect with discrimination and hate crimes relating to a young person's actual or perceived gender identity, sexual orientation, race, religion, special educational need or disability. Childnet staff interpreted this evidence as an indication that only a holistic and gender-sensitive approach involving multiple stakeholders can ensure a successful response to online sexual violence.

Building on this, deSHAME's final outcomes included some thoughtful **recommendations and practical resources** for different typologies of practitioners[70]. This entailed, first, a strong focus on **education**. Childnet constructed a toolkit[71] based on lesson plans, posters, films and guidance for schools on how to educate young people on online sexual harassment and how to best respond to it. Believing that teacher training is essential for these educational resources to be useful, Childnet explicitly recommended that teachers address the issue in a non-judgemental, supportive way. The presence of a Youth Ambassadors Board also allowed the charity to distribute these materials widely.

Second, Childnet is vocal about the necessity of providing **training and support for the police, social workers[72]** and other actors interacting with children. With this in mind, they fashioned specific resources and guidance to help law enforcement agencies and other relevant stakeholders understand barriers to reporting, how to assess a situation of online sexual harassment, and provide ongoing support for survivors, perpetrators and families. Third, deSHAME's leads have been **working closely with the tech industry and policy makers**, which they see as a key element towards tackling online abuse. This relationship has been built and maintained by seeking a place on the advisory boards of a number of social media platforms, as well as recruiting an Expert Advisory Board including voices from industry, teachers, government, police and other charities.

Finally, as well as supporting survivors, Childnet's resources offer advice to authorities and social workers on how to **work with young perpetrators**. In particular, they seek to improve our understanding of the motivations of young people, especially in cases in which youths display problematic behaviours because of the effect of other types of violence and exploitation.

Strengths and potential limitations. An important strength of Childnet's work is that it fully involves and centres its practices around **survivors** and others who are affected by online sexual harassment. Specifically, the opinions of young people provided a basis to develop resources, and useful evidence to lobby social media companies[73]. Crucially, this also served to conceptualise online sexual harassment as a phenomenon taking place in a broad range of formats, while clearly stating that each and every of these formats should be taken seriously (for example, by acknowledging that online harassment doesn't have to go viral to harm the survivor).

---

[70] See https://www.childnet.com/our-projects/project-deshame/advice-and-resources

[71] https://www.childnet.com/resources/step-up-speak-up/teaching-toolkit

[72] See https://www.childnet.com/resources/step-up-speak-up/guidance-and-training-for-schools-and-professionals

[73] See Tangen R. 'Listening to children's voices in educational research: some theoretical and methodological problems', European Journal of Special Needs Education. 2008 May 1, 23(2):157-66.

Furthermore, deSHAME rightfully **focuses on online communities**, and on ensuring that these are built as positive spaces through an active bystander approach. Childnet sees its work as targeting "not just the victims who experience it, but everyone who sees that type of behaviour going on online". Its aim is to shape a different digital culture, "based on respect, consent and trust"[74], so that less strain is put on individuals and single organisations, and virtuous collaborations are fostered in the field. Equally importantly, Childnet openly considers the **double marginalisation** faced by young people in vulnerable groups, recognising that they do not only suffer unique forms of harassment, but also encounter specific barriers to accessing support. This includes girls of colour, disabled girls, LGBTQ+ young people and others experiencing intersecting disadvantages. Whilst deSHAME's final report had relatively low numbers of BME and LGBTQ+ respondents, qualitative research was conducted to purposefully highlight and consider the voices of queer youth. Similarly, the report explicitly acknowledged that ethnic minorities might not see the police as a particularly supportive institution, which should be taken into consideration when building effective and inclusive reporting procedures.

On the other hand, due to Childnet's specific mission, it is worth noticing that its recommendations and solutions are **designed around young people only**. Whilst education is crucial to prevent any form of violence, schools play a central role in young people's education, and, in the absence of a corresponding institution for adults, more creative approaches are needed to raise awareness on DGBV in general. Equally, while the toolkit developed by Childnet can offer food for thought to GBV practitioners, the language used in materials and workshops must be age-specific. The complex ways in which DGBV affects adult women in abusive domestic relationships also require special attention, which falls outside the scope of Childnet's work.

Lastly, Childnet's advocacy strategy presents several elements of interest. In particular, **seeking space on corporate boards** is an effective way to put pressure on private sector actors, and one that is not often available to those working in the field of GBV. Due to its long-term work on children's right to digital safety, Childnet can rightfully portray itself as a crucial civil society stakeholder. However, as highlighted in our analysis of the partnership between EWL and Google, civil society advocates that work closely with corporate partners must constantly **find creative ways to retain their identity and mission** while engaging in necessary mediation work.

Lessons to be learned. A key, unanswered question that remains is the extent to which the solutions elaborated by Childnet to tackle peer-online harassment among young people, regardless of gender, can be **transferred to the field of DGBV more generally**. A first, important caveat concerns the **ways in which women and children are portrayed at societal level**. On the one hand, until relatively recently women, children and various vulnerable people were treated as 'weak' subjects in both legal and societal discourse, with the effect of denying their agency and erasing their voices. The association between these different categories also contributed to specifically infantilise adult women[75]. We must therefore be careful when equating women and children as groups deserving protection. On the other hand, as discussed, gender intersects with not only age, but also race, class, sexual orientation, and health conditions, giving rise to the need for a nuanced perspective on how DGBV affects different communities.

---

[74] Quote extracted from interview with Childnet's staff.
[75] See Huot, C.R., Language as a social reality: The effects of the infantilization of women, 2013.

That being said, the findings and resources provided by Childnet show awareness of these complexities, and can be of great interest to organisations fighting DGBV globally. The staff at Childnet intelligently **used their resources and organisational legitimacy**[76] to inform the societal debate on online abuse and to educate the general public on legal standards and good practices. As child safety is a dominant public concern, increasing awareness of the gendered nature of peer-online abuse among young people contributed to bring DGBV to public attention in the UK and internationally. Similarly well-positioned actors in other countries may use the same strategy to mobilise target-audiences on DGBV-related concerns. The role that Rajeshkumar and Proffitt played in this process can also be read as a lesson on the power that **individual women and small groups can play as social intrapreneurs**, driving change from within existing organisations.

Furthermore, a few elements of Childnet's approach could offer a useful **reference and benchmark** for other organisations working on DGBV specifically, regardless of the national context. For example, deSHAME defines online sexual harassment starting from the notion of consent (or lack thereof), which helps understand what may constitute violence, and what its impact may be, in novel and often misunderstood contexts such as online interactions. The all-inclusive nature of Childnet's work, its effort to get multiple actors involved, and its commitment to produce clear and straightforward recommendations, training and practical resources for different groups of practitioners can also be applied to DGBV as a wider issue.

Finally, some of the materials produced by Childnet could be of specific interest to women's organisations and community services. In fact, **training pre-existing support groups for women and non-binary people** is essential to meet the needs of those who experience various forms of marginality and do not have access to other services. These actors might specifically benefit from good-quality information and guidance on DGBV as a relatively new and particularly pernicious phenomenon, and combine these with their expertise on bottom-up approaches.

---

[76] See also Sinclair R. and Bolt R. 'Third sector accounting standard setting: Do third sector stakeholders have voice?', Voluntas: International Journal of Voluntary and Nonprofit Organizations, 2013 1, 24(3):760-84.

When an unprecedented problem requires a brand-new organisation: the case of UK's Glitch!

By E.M. Wroth, Ciara Taylor & Lilia Giugni

The context and the problem: racist and sexist online abuse in the UK. In the United Kingdom, gender- and racially-based digital violence is gaining increased attention in public life, with former Prime Minister Theresa May recently calling the **online vitriol directed against political and public-facing figures** "a threat to democracy"[77]. In 2018, the British Law Commission reported that 97% of UK-based malicious communication offences (online and offline) go unreported, and discussed at length the growing impact of digital abuse, its gendered nature and impact on vulnerable groups[78]. In the same year, Amnesty International revealed that abusive Tweets targeted female politicians, journalists and activists in the UK and the US on average every 30 seconds, and that black women were 84% more likely than white women to be the victims of abuse[79].

Whilst British women's groups and organisations in the cybersecurity space have gradually started grappling with the problem, the novel and complex challenges posed by digital abuse have left many feeling that **more radical and innovative solutions** are needed. This approach has been embraced by Glitch!, a growing not-for-profit organisation that seeks to end online abuse while building on intersectional feminist principles[80]. Glitch! was founded in 2017 by anti-racism and feminist activist and former Labour politician Seyi Akiwowo, as a response to the intense online abuse she had faced after a video of her speaking at the European Parliament went viral[81]. Turning that experience into a call for action, Akiwowo created Glitch! to ensure that the current rise in online abuse should only be a "glitch" – a temporary technological malfunction, and not a longstanding issue of our times.

Fuelled by Akiwowo's own experience of **misogynoir** (misogynistic and racialised) **digital abuse**, the charity's mission is informed by **intersectional perspectives, data and tools**. As she explains[82], Akiwowo felt that for far too long research on online abuse had focused on women and children, as if the two were homogenous groups, while ignoring the specific vulnerability of non-white, non-Christian, non-heterosexual and disabled women. In so doing, many of the existing enquiries had ignored the real drivers behind much of the ongoing abuse. With this in mind, Glitch! champions a more nuanced attitude to social critique, research and action surrounding digital abuse, and urges for responsible data-gathering on women with intersectional identities and for their involvement in the search for solutions.

---

[77] See https://www.theguardian.com/society/2018/feb/05/theresa-may-calls-abuse-in-public-life-a-threat-to-democracy-online-social-media.

[78] The Law Commission's report is available at: https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/10/6.5013_LC_Online-Summary-Report_FINAL_WEB.pdf

[79] See https://www.amnesty.org.uk/press-releases/women-abused-twitter-every-30-seconds-new-study

[80] See https://fixtheglitch.org

[81] For further details, see https://seyiakiwowo.com

[82] Our analysis of this case is based on multiple interviews with the founder combined with the analysis of media documents and outputs produced by the charity since 2017.

Whilst these views are increasingly shared by DGBV activists and experts internationally, what makes Glitch's case particularly insightful is the founder's resolution to **create a brand-new organisation** to address what she felt was a misunderstood and largely unrecognised social problem. In light of this, we examined the charity's challenges and achievements, as well as the transferability of its practices.

Good practice: creating a single-issue campaign organisation. Glitch's mission has progressively evolved to include three main objectives, summarised at the '3 As': **Awareness, Advocacy and Action**. This is achieved by engaging with different kinds of stakeholders (including young people and their schools, tech companies and policy makers) and attempting to shift the debate on digital violence at various levels. The 'Digital Citizenship' workshop[83], to begin with, is Glitch's flagship interactive **awareness-raising initiative, primarily aimed at young people**. It builds upon a behavioural intervention model, delivered in a creative and informal way, to help young people adopt more positive digital lifestyles. Workshops have so far been delivered to over 3,500 young people across the UK and Europe, and to 100 young European Leaders in Strasbourg. Further, Glitch! has held training sessions for 200 women in public-facing roles in the UK, Canada and Ghana, focusing mainly on digital self-care. Drawing on its workshops and training sessions, in 2019 the charity produced and distributed a 'train the trainer' toolkit[84] based on suggestions for parents, teachers, employers and other relevant actors to host helpful conversations about online abuse, which has been downloaded internationally.

Advocacy efforts aimed at policy makers, on the other hand, include Glitch!'s 'Tech Tax' campaign[85], which calls upon the UK Chancellor of the Exchequer to ringfence at least 1% of the new UK Digital Services Tax, announced 29th October 2018, to efficiently and effectively combat online abuse. Specifically, Glitch! recommends that, through no negative deficit, funds should be pledged to: first, enforcing existing legislation on online abuse and increasing police resources; second, educating the public on the importance of good online citizenship[86]; and third, empowering individuals and civil society organisations working in the field.

Furthermore, Glitch! is a vocal critic of social media companies that refuse to be held accountable for their online content in the same way mainstream media would be. Accordingly, the organisation advocates for a change in the UK's self-regulatory digital approach, and more stringent regulation for social media platforms. It has its sights on the Australian regulatory model, whereby an E-Safety Commissioner works alongside social media companies and regulators, tackling issues such as wellbeing and health as well as online violence against women (see our Australian case study). Building on this, the charity has produced **a set of initial recommendations for tech actors** such as YouTube and Twitter,

---

[83] See https://seyiakiwowo.files.wordpress.com/2019/06/glitch-digital-citizenship-memo.pdf
[84] See https://tedxlondon.com/attend/beyondborders2019/speakers/SeyiAkiwowo
[85] https://fixtheglitch.org/tech-tax-campaign/
[86] Glitch's notion of digital citizenship is built on definitions borrowed from the Council of Europe and the Australian Curriculum. These encompass two key elements, digital rights and digital responsibilities of both individuals and institutions. On the one hand, individuals are seen as entitled to safely and freely engage in online spaces, based on a clear understanding of existing laws and parameters for positive online interactions. On the other hand, digital responsibilities involve understanding expectations and behaviors related to navigating online spaces. These include enacting active bystander interventions, practicing respectful online etiquette, positive engagement with digital technologies, and not misusing them to disadvantage others.

based on the experiences of survivors of online abuse and aiming at building safer digital platforms. Its main propositions revolve around abuse prevention through deterrence, the establishment of transparent regulations and effective reporting processes, as well as reasonable retribution practices for online abusers and effective communication between digital companies and users.

Meanwhile, the charity works to give visibility to its advocacy initiatives and proposed plan of actions in multiple ways. This has included, for example, national and international talks, Twitter conversations, collaborations with Amnesty International, other established charities and well-known public figures, media work[87] and private meetings with tech companies and third sector organisations' senior staff.

Strengths and potential drawbacks. Since its foundation, Glitch! has garnered both national and international praise. Akiwowo has been invited to Number 10 Downing Street and to the 38th United Nations Human Rights Council on Online Violence Against Women[88], and has been nominated 2019 Digital Leader of the Year[89]. Through workshops and media initiatives, Glitch! has effectively engaged with numerous constituencies. Its work has been recommended as best practice in a recent **European Parliament** report on cyberviolence[90], and featured in **Amnesty International**'s Write for Rights campaign. The charity's recommendations around online racism and intersectionality have also been adopted by the UN Human Rights Council. The UN report including Glitch!'s recommendations will be presented at the United Nations in New York on 30th October for adoption. As such, it can be considered one of the most active and visible UK-based organisations working against online abuse.

Glitch!, however, must deal with all the **difficulties typically faced by a small organisation in its start-up phase**. To begin with, financial sustainability is a challenge for socially minded ventures that, while having to cover their costs, are committed to make their activities freely and widely accessible. At a time where funding for human rights and violence prevention activities is scarce and competitive, securing sponsorship and charitable grants requires considerable time and energy. More established organisations with a broader mission, on the other hand, are often able to devolve part of their budget to novel projects.

Secondly, the charity's work and 'brand' is closely tied to Akiwowo's figure and personal story. While the credibility provided by an inspirational founder is an asset for any start-up, this poses problems in terms of both scaling and transferability. At the time of writing, Glitch! can count on the support of a few volunteers and many allied organisations (including established actors such as Amnesty International), but it still heavily relies on its **founder's personal resources and ability to juggle her many commitments**, ensuring both Glitch's long-term efficacy and its day-to-day functioning. This is particularly challenging considering that those

---

[87] See, for example, https://www.theguardian.com/profile/seyi-akiwowo
[88] https://fixtheglitch.org/2018/06/21/founder-director-glitchuk-seyi-akiwowos-intervention-notes-at-un-human-rights-council/
[89] https://digileaders.com/the-7th-digital-leaders-100-awards-2019-is-won-by-bame-women-in-tech/
[90] http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

involved in the project are acutely aware that DGBV can only be addressed at multiple levels and by continuously liaising with different stakeholders[91].

Finally, it is worth noticing that, like many feminist, anti-racism and DGBV violence activists and groups, Glitch! and its founder **remain a target for Internet abusers**, which has – understandably – various emotional and professional repercussions.

Lessons to be learned. Bearing in mind all these caveats, several lessons can be learned from Glitch's trajectory and accomplishments. First of all, this case epitomises **the power of small, single-issue advocacy organisations**, which – combining specific expertise and the ability to strategically occupy a given space in the public discourse – can educate and mobilise different target audiences. Secondly, it demonstrates how DGBV **survivors are best placed to elaborate good practices** that fit their own community and educate relevant constituencies on the problems they face. Thirdly, it proves how **relatively low-cost training and freely accessible materials can effectively inform awareness-raising efforts**, while showcasing the importance of applying a feminist intersectional paradigm to online violence work. Importantly, these last two considerations apply not only to specially created, brand-new organisations, but may also be of interest to other actors in the digital violence prevention space.

At the same time, policy makers, charitable foundations and other third-sector funders may want to extrapolate inputs from this case to reflect on how to best support good practices in this area. Developing both **grants and incubation- or acceleration-like initiatives for ventures that incorporate social entrepreneurial elements** (including training services) may be of great help to single-issue organisations working in this field. It may also allow more established ones to invest in new streams of work and prioritise DGBV. Finally, Glitch's collaborations with Amnesty International and other established actors offer a useful example of how **organisations of different sizes might join forces and combine complementary expertise** to raise public awareness of DGBV.

---

[91] See Weber, C., Kröger, A. and Lambrich, K., 'Scaling social enterprises–a theoretically grounded framework', Frontiers of Entrepreneurship Research, 2012, 32(19), p.3.

Special testimony feature

The power of grassroots initiatives: lessons from survivor-led research in Romania

By Venera Dimulescu

The context and the problem. If you take a look back into the recent history of my country, you'll understand that Romania is a place still haunted by old social habits and hierarchies. Communist dictatorship brought hard times for women with an anti-abortion law supposed to increase the population and make Romania big and prosperous[92]. After the Revolution, there were several attempts to introduce gender studies programmes in academia. One of them, from the National University of Political Studies and Public Administration, was particularly successful and brought up generations of feminists who fought to end domestic violence. Meanwhile, the Romanian Orthodox Church, several conservative NGOs and politicians are spreading false information about sexuality education. They are trying to ban it from schools and punish the teachers who disobey[93]. At the same time, over the last decades, domestic violence has been the most visible issue in Romania's struggle for gender equality. In the '00s, numerous scholarships helped journalists report on this subject and make the problem visible nationwide. But the backlash pushed by religious extremists and conservative politicians makes it hard for activists and reporters to do their job. This year, for example, the city council of Bucharest withdrew the funding for one of the most important shelters for victims of domestic violence. The centre was eventually closed in 2019[94].

Good practice. When I started a project on so-called **revenge porn** in 2016, there was no data about online violence involving Romanian adults, regardless of gender. However, there were several statistics on cyberbullying among children and teenagers, with a brief mention of the practice of sexting. 17.6% of children between 10 and 14 living in rural areas were sending nude photos of themselves in 2015[95] and only 2.9% were sexting in urban areas. Two years later, 80% of Romanian teenagers claimed they had been victims of cyberbullying in their lifetime[96].

Back in 2016, as an **academic researcher**, I had little to no information about non-consensual pornography in my country. I knew what the international theoretical context for the phenomenon might have been, but I had no idea how Romanians dealt with this problem. So

[92] http://www.analize-journal.ro/library/files/numarul_9/9_9_daniela_draghici_149-158.pdf

[93] https://www.digi24.ro/stiri/actualitate/politica/proiect-adoptat-de-senat-pedepse-pentru-profesorii-care-fac-educatie-sexuala-fara-acordul-parintilor-916951

[94] https://www.asociatia-anais.ro/stiri/centrul-de-gazduire-regim-de-urgenta-destinat-victimelor-violentei-domestice-casa-invicta-se

[95] https://oradenet.salvaticopiii.ro/docs/raport_cercetare_safer_internet_2015_web.pdf

[96] https://economie.hotnews.ro/stiri-it-22137645-studiu-bitdefender-80-dintre-adolescenti-romani-fost-hartuiti-internet-aspectul-fizic-pasiunile-situatia-materiala-sunt-principalele-motive.htm

I started searching for **personal narratives** that would help me understand the issue at a grassroots level. At that time, in 2016, I was part of a **local feminist NGO**, Centrul FILIA, and with their help I organised a few **classes on digital violence awareness** in high-schools and a lecture at a public library in Bucharest[97]. Those were the first steps ever taken at a national level to combat non-consensual pornography in Romania. It was at that point that I found out how this type of online abuse had reached children as young as 10 years old. Talking to school pupils, I learned that there is a clear gender difference when it comes to digital violence: boys were rather the victims of hacking, while girls were bullied for their looks and physical features in general.

I wanted to dig deeper into the problem so I shifted to **journalism** to search for personal stories of victims and oppressors[98]. After two years of research, I published three **case studies** from the seven I had documented. Two of them are currently online, the third is still in progress. Each story provides a new perspective on the same issue. The first episode shows how underage victims deal with a whole community of aggressors. It is the story of a 15-year-old girl who had been further punished by her peers – both minors and adults - for being a victim of a series of cybercrimes. Her private correspondence had been hacked by her best friend and some explicit videos of her masturbating had been spread throughout her town and the villages surrounding it. This was a serious case of child pornography, involving several criminal offences, which was left unresolved as the perpetrators were excused and the victim was blamed and punished by a public institution: her very own high-school[99]. The main causes for this injustice were a lack of knowledge regarding digital rights, legislation and sexuality education, as well as severe forms of misogyny and victim blaming that have been practiced for centuries in the Romanian society.

The second article is a two-year documentation of the efforts of an adult victim to make her perpetrator legally responsible for his abuse. Her ex-lover had published non-consensual nude photos of her online, in order to humiliate her and ruin her social life. He had harassed her on the phone for one month and encouraged her to commit suicide. He had grown up in a well-educated family, and was using his parents' wealth and social status to increase the weight to his threats. At the moment of writing, the survivor's battle has been taking place for two years, and on two fronts: with the perpetrator and with the police, who blamed the victim and belittled the abuse after she had filed a complaint[100]. The story describes a cultural quest for our society as a whole, to understand that violence committed by the intellectual elite is still violence and it should be addressed as such.

The project's personal costs and its positive outcomes. After I published the article, the perpetrator of the second case I covered found himself allies in the Romanian Incels (an online community of **men's right activists** holding severely misogynistic positions). He reached out through forums and Facebook groups to online alt-righters, who spread fake news and conspiracy theories. They started an online campaign to discredit and humiliate myself and the case victim. They published private information about the victim and abused her with sexualised slurs, whereas they sent me hateful messages in which they threatened me of

---

[97] See https://www.facebook.com/events/574458852717005/

[98] The author's articles are accessible here: https://casajurnalistului.ro/author/venera/

[99] The first story in the project is accessible at https://casajurnalistului.ro/naked-pictures-viral/..

[100] The second episode is available at https://casajurnalistului.ro/supreme-humiliation/.

physical violence and called me a "Communist" and a "frustrated radical feminist". They tried to turn the public discussion on revenge porn into an ideological fight against the "extreme left forces", as I explained in a video reportage on how online abuse perpetrators' networks of supporters are formed.

Meanwhile, two politicians from different political parties started working on **drafts on an anti-revenge porn law**. The debates were not public, yet a Romanian senator (who had been amongst the first ones to work on a bill proposal on this topic) invited me to **discuss the draft** alongside activists, politicians and members of the Criminal Investigation Department. As a result, she proposed to amend the existing privacy law by inserting an additional article, by explicitly covering non-consensual pornography practices[101]. The law has recently been passed by the Judicial Commission.

Lessons learned. In my effort to make non-consensual pornography a relevant issue in the Romanian public discourse, I adopted a **specific strategy**. My editor in chief, Vlad Ursulean, and I thought about what we could do to reach the people who needed the information the most, and came up with a few key points and a plan of action that might be helpful to other working in the field.

First, we knew that Romania's televisions and mainstream newspapers were suffocated by overly emotional or sensationalist language. Domestic abuse is often reported as "acts of love" and in the few revenge porn cases exposed, the victims are highly sexualized and presented as "hot chicks who went viral". In my articles, instead, I used a **"stick to the facts" approach**: I made use of an **accessible language** so that the story reached diverse groups of people, regardless their education and knowledge on human rights. I also focused on the facts in order to avoid worn-out and sensationalist discourse, and so that the readers could understand that abuse might happen to anyone and **feel more connected with the victim**. In the second story, I focused on the aggressor and the way he used his parents' social status and political power to get rid of the responsibility he bears for his deeds. In a society where physical, emotional and digital abuse are normalised, we need to name social roles and the impact they have on our relationships. The victim-perpetrator dynamic is extremely important to assess, to avoid falling in a grey area which might make the abuse hard to define and to tackle.

Secondly, after the publication, I made sure to reach what I considered the **key audiences** for each case. In order to ensure that my key message penetrated outside our usual readers' social bubble and my own activist and social media community, I **emailed the articles to public institutions**, NGOs, public schools, politicians and youth magazines. As a result, I was invited at the Romanian Parliament to speak with several politicians and inform them about online violence[102]. I also spoke on the subject at a live show for Elle Magazine[103], a mainstream women's publication, and in an interview for a popular sexuality education NGO[104]. I distributed **flyers** on the project on the street, and talked to as many people as possible face to face. My colleagues helped by producing **posters** to be exhibited in important public spaces

---

[101] See https://legeaz.net/noul-cod-penal/art-226
[102] More details are available here: https://www.facebook.com/venera.dimulescu/posts/10211888604754680
[103] See https://www.elle.ro/video/ellenutace-sexting-si-pornografie-595590/.
[104] See https://www.youtube.com/watch?v=l0Y_HjEjKVI.

in Bucharest and several other Romanian cities[105]. In addition to this, I went back to deliver **talks in high-schools**[106] and spoke to teenagers and their teachers about revenge porn and encouraged them to comment upon my article, stimulating their reactions and fostering a debate. Finally, I collected and **posted online the observations** I drew during these interactions, aiming to also reach a diversified online audience.

> **GenPol's reflections.**
> Believing, as discussed, that survivors' voices should be at the very centre of any efforts to combat gender-based violence, we chose to integrate this case study as a special testimony feature. In so doing, while keeping the paper's focus on the specificities of the practice under exam, its strengths, potential drawbacks and transferability, we published this account in first person and did our best to showcase the author's personal considerations. To this, we would like to add a few extra reflections on the lessons that others may learn from this example of multifaceted and very effective in-depth reporting. On the one hand, Venera Dimulescu's inspirational story offers precious insights into how **progressive media can work with activists, experts and survivors** to help shift the conversation on DGBV[107]. It also sheds light on the mechanisms that may lead bottom-up initiatives to gain a national profile and provide a basis for policy reform and educational interventions. Beyond Dimulescu's expertise and great dedication, her editor and interlocutor in the Romanian Senate also epitomise the way passionate individuals can push for social change from inside established organisations. On the other hand, this case study exemplifies the **risks that feminist work entails**[108], and the need to more effectively support survivors, feminist researchers and activists, who – like Dimulescu and her collaborators – remain under attack and exposed to re-victimisation as well as legal and economic attacks. Lastly, it is also significant that Dimulescu transitioned **from academia to journalism**, feeling that this could allow her to reach out to a broader audience. Academic and research institutions may want to draw on this to elaborate more creative ways to make scholarship on gender-based violence widely accessible[109] beyond academia.

---

[105] Posters can be visualized here:
https://www.facebook.com/casa.jurnalistului/posts/1846083405462980?__tn__=H-R
[106] See:
https://www.facebook.com/casa.jurnalistului/photos/a.225285044209499/1848962941841693/?type=3&theater
[107] See, for example, Nichols, A.J., 'Gendered organizations: Challenges for domestic violence victim advocates and feminist advocacy', Feminist Criminology, 2011, 6(2), pp.111-131.
[108] See Nuñez Puente, S. 'Feminist cyberactivism: Violence against women, internet politics, and Spanish feminist praxis online', Continuum: Journal of Media & Cultural Studies, 2011 1;25(03):333-46; Lewis, R., Rowe, M. and Wiper, C., 'Online abuse of feminists as an emerging form of violence against women and girls', British journal of criminology, 2016, 57(6), pp.1462-1481.
[109] See, for example, Sherman, F.T. and Torbert, W.R. eds., Transforming social inquiry, transforming social action: New paradigms for crossing the theory/practice divide in universities and communities (Vol. 4), Springer Science & Business Media: 2000.

What about tech-led solutions? Of software and human moderators

By Chiara De Santis

The context and the problem: the dilemma of online content moderation. The amount and variety of User Generated Content (UGC) produced each day in the world has reached proportions unimaginable even a few decades ago. As a consequence, moderation of UGC has become one of the great challenges of the digitalised society[110]. Tech giants as well as medium- and small-sized platforms in a wide range of sectors, from mainstream media to e-commerce and user-centred forums, are currently **under pressure to protect the safety and rights of their users by keeping improving their content guidelines, moderation and take down policies**[111]. In particular, in spite of increased public attention and intense criticisms from civil society organisations, hateful, violent and **harmful content targeting women, minorities and vulnerable groups** is still shared globally on a daily basis.

At the same time, as has been emphasised elsewhere[112], the strictest examples of censorship (i.e. forbidding the use of certain words or hashtags) appear both ineffective in filtering violent messages and unreasonably restrictive of democratic and respectful discussions. In fact, **the complexity of online content moderation lies both in the limits of the tools currently employed by digital companies and in the multifaceted nature of UGC.** First, potentially violent contents can often be identified and properly moderated only when appropriately **put into context**. Second, the **variety of UGC formats poses further challenges**[113]. Video content, for example, requires each frame to be checked, while memes need to be evaluated on the basis of the interaction between text and images. Similarly, real time streaming also necessitates live moderation.

The limits and costs of current solutions. As most digital platforms continue to rely heavily on human intervention, recent investigations have shed light on the unacceptable toll of human moderation. Whilst tech companies often resist efforts to monitor violations of moderators' rights**, growing evidence shows that the constant exposure to triggering content causes serious psychological damages**, including PTSD-like symptoms[114]. Moreover, moderators (who are generally recruited in emerging economies and work as subcontractors)

---

[110] See, for example, Accenture, Content Moderation, 2017, available online at:
https://www.accenture.com/ie-en/_acnmedia/PDF-47/Accenture-Webscale-New-Content-Moderation-POV.pdf
[111] See, for example, Nanonets, Content Moderation in 2019: Human vs AI, available online at:
https://nanonets.com/blog/nsfw-content-moderation-in-2019-humans-vs-ai/
[112] See Stanford Daily, The mistreated moderators and the pervasive violence of the Internet, available online at https://www.stanforddaily.com/2019/03/06/me-ll-mistreated-moderators-and-the-pervasive-violence-of-the-internet/
[113] See, for example, Cambridge Consultants, Use of AI in online content moderation, available online at:
https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf
[114] The Verge, The Secret Lives of Facebook moderators, available online at:
https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona; Arsht, A. and Etcovitch, D., The Human Cost of Online Content Moderation, available online at : https://jolt.law.harvard.edu/digest/the-human-cost-of-online-content-moderation

may be **required to meet unreasonable quotas**, which increases their mental health risks. Finally**, lack of clarity in tech companies' community standards**, as well as insufficient training and lack of sensitivity to cultural differences between staff and users worldwide, all add to these heavy costs[115].

On the other hand, policy makers and digital leaders often refer to AI-based solutions as the future of moderation[116]. In an ideal scenario, they suggest, algorithms will be able to teach themselves to edit any kind of content, keeping a pace as fast as that of the evolving formats of UGC and protecting employees from psychological harm. Such expectations, however, do not seem entirely realistic[117]. Considering both the current state of AI development and the growing complexity of UGC, it is **hard to imagine** how moderation processes might **become both completely automated and totally successful in the nearest future**.

Good practices and future directions. As a result, **mixed systems utilising both algorithmic and human intervention seem more attainable in the short/medium term**, and AI advancements can be more reasonably expected to provide **further support and protection to employees.** Enhanced algorithmic solutions could, for example, **filter violent content with increasing accuracy**, reducing human exposure to potential triggers. At the same time, it is imperative that digital platforms ensure better working conditions to their workers and contractors, improve policies to minimise the distribution of abusive UGC, and keep up with the rapid changes in online content design and diversity.

A few examples of general guidelines, of interest to both the tech industry and lawmakers working to regulate this sector, have been provided by the **Transatlantic High-Level Working Group on Content Moderation Online and Freedom of Expression**[118]. This high-level commission, which includes government representatives, legislators, corporate and policy experts from the European Union, Member States and the USA, published several reports and working papers, ending in the following recommendations: i) specific harms that are the object of content moderation should be **clearly defined**; ii)**transparency must be built in** both by governments and platforms, so that the public and other stakeholders can more accurately evaluate the impact of moderation; iii)due diligence safeguards have to be issued to give authors of taken-down UGC clear and timely recourse for appeal; 4) all stakeholders must understand the **risks of overreliance on artificial intelligence,** especially for context-specific issues like hate speech or disinformation, and include an adequate number of human reviewers to correct for machine error.

---

[115] See, for example, Cambridge Consultants, op. cit.

[116] The Verge, AI is an excuse for Facebook to keep messing up, available online at: https://www.theverge.com/2018/4/13/17235042/facebook-mark-zuckerberg-ai-artificial-intelligence-excuse-congress-hearings;

[117] See The Verge, Why AI can't fix content moderation, available online at: https://www.theverge.com/2019/7/2/20679102/content-moderation-ai-social-media-behind-the-screen-sarah-t-roberts-vergecast

[118] Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, press review, June 2019, available online at: https://www.annenbergpublicpolicycenter.org/governments-platforms-fallen-short-trying-to-moderate-content-online/

Further lessons can be learned from the ***Guardian*'s Community Standards**[119]. In fact, the way in which the British newspaper moderates readers' comments on its website are among the most virtuous examples of how to achieve a constructive space for debate and exchange of ideas, while protecting the rights and safety of all users. Specifically, comments on the news-site are blocked according to well-defined criteria, either because they break the law or as they are 'considered abusive to some degree, or otherwise disruptive to the conversation (they are, for example, off-topic)'. In a 2016 special feature[120], *Guardian* journalists analysed their website's own moderation practices, focusing in particular on what was considered to be 'disruptive behaviour'. The research, however, also provided evidence of blocked comments that constituted either a form of 'author abuse' and *ad hominem* attack towards journalists and other users, or 'dismissive trolling' (sadly but unsurprisingly, **women journalists were proven to be specifically targeted**). In so doing, the piece clearly explained how all moderation decisions were made not on the basis of the moderators' own tastes or ideas, but strictly following the Community Standards and based on the idea that **what is (or should be) unacceptable offline, such as sexism, racism, homo-transphobia or any type of hate speech, should be equally considered unacceptable in the digital space.**

Finally, it is equally crucial to seek good practices with the purpose of guaranteeing healthy working conditions for moderators. It is worth noticing that tech giants are reacting to the combination of public outrage and pressure by unions and other advocates, and are currently scoping possible solutions. Facebook, for instance, announced it will **end daily post quotas**, raise the wages of U.S. moderators, and promised unlimited access to counselling for employees around the world. Similarly, YouTube has declared that their moderators worldwide have "regular" access to counselling, and Twitter is said to have **required that its contractor companies also offer additional psychological support to workers after work**[121]. An interesting case is that of the **Technology Coalition**[122], formed in 2006 by world's leading tech actors with the mission of eradicating online child exploitation. While supporting both emerging and established companies' efforts to **detect and report images** of child sexual exploitation and other predatory practices, the Coalition also guides and instructs them on how **to handle, classify, and report abusive material** and ensure a "supportive, resiliency-focused environment for content moderation staff members". Importantly, such efforts could be extended to the field of DGBV prevention.

It is crucial, however, that these attempts are coordinated, strengthened, and designed to **take into account the different legislations and contexts** of the countries in which the majority of content moderators work, while maximising the advantages of algorithmic tools. Digital companies must protect the digital (and human) rights of women and vulnerable users, but this cannot happen at the cost of workers' rights violations.

---

[119] The Guardian, Community Standards and Participation Guidelines, available online at: https://www.theguardian.com/community-standards

[120] The Guardian, The Dark Side of Guardian Comments, 2016, available online at: https://www.theguardian.com/technology/2016/apr/12/the-dark-side-of-guardian-comments

[121] The Washington Post, 'Content moderators at YouTube, Facebook and Twitter see the worst of the web — and suffer silently', July 2019, available online at: https://www.washingtonpost.com/technology/2019/07/25/social-media-companies-are-outsourcing-their-dirty-work-philippines-generation-workers-is-paying-price/

[122] For example, see online at: https://www.technologycoalition.org/

Part 3

GenPol recommendations

Recommendations for policy makers, legal and law enforcement agencies

As epitomised by our Australian case study, **new criminal and civil legislation** is urgently needed to address **specific legal loopholes** (instances of image-based abuse could have not been prosecuted in Australia without the recent legislative intervention). This may apply, for example, to cases of digital voyeurism and non-consensual or unsolicited pornography. Yet, as we saw, in many legal systems worldwide **existing provisions on stalking, hate speech, threats, privacy and harassment in the workplace** can be effectively applied to persecute and respond to DGBV cases.

Three courses of actions are, therefore, truly imperative. First, **legal and law enforcement personnel must be trained to recognise the gendered and intersectional components** of online violence, and must, accordingly, implement national and international legal sources (starting from the **Council of Europe Istanbul Convention** on violence against women, which -as has been suggested elsewhere[123]- can be interpreted as covering DGBV cases). Second, tech companies should be pushed to adopt **more effective reporting mechanisms, take down procedures and moderation techniques, as well as more transparent data policies and internal gender equality commitments**. In particular, as social media and Internet intermediary platforms are increasingly utilised and regarded as a source of information by millions of people globally, they should ensure that content shared by their users does not violate women's digital and human rights. Third, as **educational intervention** is crucial to prevent all forms of abuse, DGBV-related issues must be taken into account in **Sexuality and Relationship Education and other appropriate statutory curricula**. In order to make sure that educational programmes successfully unpack and **counteract the sexist stereotypes** and discriminatory attitudes that inform violence in all its manifestations, **experts and specialised charities** and practitioners should be involved in both curricula and teaching material development, as well as actual teaching and training of teachers, parents and other figures with pastoral care responsibilities. Our analysis of Childnet's deSHAME Project in the UK showcases the benefits of that involvement. The creation of a **consulting body or taskforce** especially entrusted to advise lawmakers and other critical stakeholders on DGBV-related matters (once again borrowed from the Australian case study) is another example of good practices in this area. As illustrated by both our Romanian and British cases, however, it is essential that the **voices of DGBV survivors** (and of the organisations that support them) are centralised during consultation efforts.

Recommendations for employers, trade unions, professional associations and E&D teams

Training on DGBV issues is needed not only for the youth and those with teaching responsibilities, but for different categories of professionals and organisations. As we increasingly witness examples of digitally facilitated abuse and exploitation in workplaces and

---

[123] See, for example, Jurasz, O. and Barker, K., Submission of Evidence on Online Violence Against Women to the UN Special Rapporteur on Violence Against Women, its Causes and Consequences, 2017, Dr Dubravka Šimonovíc. United Nations.

universities, and more and more women are attacked on the Internet as a result of their professional activities, professional associations, trade unions, HR and Equality & Diversity divisions should both **train their personnel and raise awareness among their members** and beneficiaries around DGBV, its causes, effects and legal ramifications. More generally, gender equality and intersectional issues should be mainstreamed in all areas of an organisation's work.

Good quality **toolkits and resource packages** (especially if freely downloadable and incorporating an intersectional feminist perspective, such as the materials produced by European Women's Lobby, Glitch! and Childnet) are a cost-effective way to spread information and best practices on DGBV and gender-based harassment in the workplace. **Online events** (like the conference organised by European Women's Lobby in 2017) can also be used to connect experts and practitioners with workplaces and other interested parts. Importantly, though, such outputs should be **co-produced with experts and women's rights organisations' practitioners**, as well as translated and adapted to different organisational and cultural contests. Incorporating a focus on **bystander approaches** (which assumes that everyone might witness a violent interaction online, and should therefore know how to respond to it) is another useful and non-judgmental strategy to convey the message that DGBV is everyone's business.

Finally, workplaces and professional associations should be ready to **provide employees and members who experienced online violence with appropriate support** (once again, collaborations with DGBV specialists and a good knowledge of the resources that they produce may be particularly useful). This especially applies to fields where women (generally in public-facing roles) are particularly exposed to online violence. For example, **political parties, media companies and news agencies** must be prepared to provide female politicians, reporters and contributors with training, protection and support.

Recommendations for the tech industry

As we saw, gender inequality and sexism within the tech industry contribute both directly and indirectly to reinforce DGBV. Tech companies can thus help tackle online violence by introducing both **equality and diversity policies, training and programmes**, and **specific initiatives surrounding women's and digital rights and DGBV**. The work carried out in the public sector by Childnet, European Women's Lobby and Glitch! shows that **cross-sector partnerships** may be particularly effective, especially if they entail training, policy advice, brainstorming around technical solutions and some form of financial and logistical support devoted to third sector initiatives. Whilst Corporate Social Responsibility projects should not translate into short-term PR operations, **support from the tech industry** can meaningfully contribute to grassroots gender equality initiatives.

As illustrated by our last case study, various **software-based mechanisms** can be used by social media platforms and Internet intermediaries to suitably moderate their content and ensure that the safety and rights of their users are respected. Yet employers should be aware of the impact that moderation work has on staff, and effectively use AI solutions to limit exposure to traumatic content as much as possible and provide moderators with adequate

support. Finally, as Childnet's and European Women's Lobby case studies demonstrate, **appointing DGBV experts as board members** and identifying **appropriate contact points** to liaise with third sector partners are useful strategies to ensure mutually beneficial collaborations.

Recommendations for media companies and research institutions

The coverage of DGBV and the language that is used around it crucially contribute to frame societal discourse. As suggested by our Romanian case, **in-depth reporting** that is both rigorous and sensitive to the needs of survivors is key to create public awareness. However, mainstream media often concur to reinforce gender stereotypes and discriminatory stances through inaccurate recording, misleading language and victim-blaming attitudes. Therefore, **specially designed training** must be provided for media personnel, while national and international authorities must monitor and ensure **the safety of female journalists and the levels of gender inequality** in the field (as discussed, male- and white-dominated fields tend to nurture sexist attitudes and to trivialise various forms of harassment). **Moderation softwares** (such as the one used by the British Guardian) and other reporting and take down mechanisms must be also applied to sanction abusive comments and protect both readers and contributors.

Research institutions should contribute to the fight against DGBV through their research efforts. Largely understudied aspects, such as the **online abuse of disabled people** and the ways in which **digitalisation contributes to the economic exploitation of women**, deserve specific attention. In addition, universities should protect **female academics, students** and other employees and beneficiaries belonging to vulnerable groups from online violence and sexist discrimination. In particular, they should make sure that **investigations of DGBV include the voices of practitioners and survivors** and lead to the **(co-)creation of research outputs** that may be of use to these communities. Research findings should also be **effectively communicated and made widely accessible beyond academia** (a few lessons can be learned with this respect from our Romanian case). Finally, academic institutions can also **leverage their research budget and social capital** to support the work of DGBV practitioners and inform policy making in this area (see, for example, the role played by research efforts in our EWL case).

Recommendations for activists, women's and human rights organisations, trainers and educators

Individuals and organisations that seek to tackle and create awareness on DGBV should first of all bear in mind that an **intersectional** approach is key. As shown by all our case studies, specific groups are particularly vulnerable to online violence as well as to other forms of abuse, and their voices and needs should play a central role in advocacy and educational projects at any level.

Secondly, **collaborations between organisations and groups of different sizes and with complementary missions** might help reach diversified target audiences and overcome budget

limits and logistical difficulties. Two of our case studies illustrate this point: Glitch's collaboration with Amnesty International and advocacy work across various IGOs, and Venera Dimilescu's outreach initiatives involving media, political elites and women's organisations. Specifically, human and women's rights groups can benefit from the **specific expertise of those working exclusively on online violence**, while contributing to give support and visibility to their projects. EWL's and Chilldnet's cases also exemplify how creative funding strategies and **exchange of skills, training and guidance between organisations from different sectors** can both spread information around DGBV and help brainstorm potential solutions.

Practitioners as well as educators and trainers should also **familiarise themselves with existing research, training and teaching materials on DGBV** (including the ones included in this paper's selected bibliography and on the websites of the organisations we examined). While existing good quality resources often exist in English language, a cost-effective way to inform one's work is to devote funding to **culturally-sensitive translations**, and to **skills and information exchanges with experts** and sister organisations.

Finally, effective advocacy strategies might include the selection of **ambassadors** who are likely to connect with one's target audience, the identification of **key gate keepers** in tech companies, political elites and media, and of **local community partners**.

Recommendations for organisations supporting survivors and practitioners (and survivors themselves)

Experiencing DGBV implies huge personal costs in terms of mental and physical health, as well as social, professional and economic repercussions. It is thus imperative to devote **funding and strategic planning to strengthen survivors' support networks**, and provide them with **appropriate legal and psychological counselling**. **Third sector funders, grant-giving organisations and private sector funders** might want to explore the possibility of financing: (i) **research projects** on digital rights and online violence, including the co-creation of resources such as **prevention guidelines, training for legal, medical and women's rights experts, masterclasses** on DGBV for various categories of professionals; (ii) **specific projects ran by consortiums** of established charities, DGBV experts and community actors, and with an intersectional and survivors-centred focus; (iii) single-issue **grassroots and educational campaigns**.

Organisations specialising in domestic and sexual violence, **mental health charities and legal and medical professional associations** should also offer **specialised training** on DGBV, its impact and legal context, and include survivors of online violence in their **pro-bono** initiatives.

Finally, we hope that survivors may also benefit from the resources listed in this paper, particularly in the final section of our bibliography. With this in mind, we included both the toolkits and resource packs examined in the paper, and further guidelines on **digital rights, safety and self-care.**

Selected bibliography and other resources

Key academic and policy literature

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

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

Atalanta, (Anti)Social Media. The benefits and pitfalls of digital for female politicians, 2018, available at: https://www.atalanta.co/news/2018/3/13/antisocial-media-the-benefits-and-pitfalls-of-digital-for-female-politicians

Cammaerts, B., ICT-usage among transnational social movements in the networked society - to organise, to mobilise and to debate, 2005, available at: https://core.ac.uk/download/pdf/93297.pdf

Council of Europe, CyberCrime Convention Committee, Working Group on cyberbullying and other forms of online violence, especially against women and children, 'Mapping study on cyberviolence', 2018, available at: https://rm.coe.int/t-cy-2017-10- cbg-study/16808b72da.

Citron, M., Hate Crimes in Cyberspace, Harvard University Press: 2014.

European Commission, 2018 Report on equality between women and men in the EU, 2018, available at:http://ec.europa.eu/newsroom/just/document.cfm?doc_id=50074

European Institute for Gender Equality, Cyber violence against women and girls, 2017, available online at: http://eige.europa.eu/rdc/eige-publications/cyber-violence- against-women-and-girls

European Parliament, Empowering women and girls in media and ICT - key for the future, 2018, available at http://www.europarl.europa.eu/RegData/etudes/PERI/2018/606788/IPOL_PERI(2018)606788_EN.pdf

European Parliament, Cyber violence and hate speech online against women, Study for the FEMM Committee, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union, PE 604.979 – September 2018.

GenderIT.org: Feminist reflection on Internet policies, last accessed October 2019, available at: http://www.genderit.org/

ITU, Gender Equality and the Empowerment of Women and Girls through ICTs, 2018, available at:http://www.itu.int/en/action/gender-equality/Pages/default.aspx

Jane, E.A., '"Back to the kitchen, cunt': speaking the unspeakable about online misogyny', Continuum: Journal of Media & Cultural Studies, 2014, Vol. 28, No. 4, 558–570.

Kamal, M., Newman, W.J., 'Revenge Pornography: Mental Health Implications and Related Legislation', Journal of American Academy of Psychiatry Law, 2016 Sep;44(3):359-67

Noble, S. Algorithms of Oppression. New York: NYU University Press: 2018

Pew Research Center, Online Harassment, 2014, available at: http://www.pewinternet.org/2014/10/22/online-harassment/

Uhl, C. A., Rhyner, K. J., Terrance, C. A., & Lugo, N. R. (2018). 'An examination of nonconsensual pornography websites', Feminism & Psychology, 28(1), 50–68.

UN Broadband Commission for Digital Development, Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call, 2015, available online at: http://www.unwomen. org/-/media/headquarters/attachments/sections/library/ publications/2015/cyber_violence_gender%20report. pdf?vs=4259

UNESCO, Building Digital Safety for Journalists, 2015, available at: https://ipi.media/online-abuse-of-journalists-has-deep-psychological-impact-experts-say

Web Foundation, Women's Rights Online Digital Gender Gap Audit, 2016, available http://www.europarl.europa.eu/RegData/etudes/PERI/2018/606788/IPOL_PERI(2018)606788 _EN.pdf

Worsley, J. D., Wheatcroft, J. M., Short, E., & Corcoran, R., Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses. SAGE Open.: 2017

Useful toolkits and resource packs

Association for Progressive Communication, ICTs for Feminist Movement Building: Activist Toolkit, 2018, available at: https://www.apc.org/en/pubs/icts-feminist-movement-building-activist-toolkit

European Women's Lobby, #HerNetHerRights. Resource Pack on ending online violence against women & girls in Europe, 2017, available online at: https://www.womenlobby.org/IMG/pdf/hernetherrights_resource_pack_2017_web_version. pdf

Fix the Glitch Toolkit, 2019, available online at: https://fixtheglitch.org/toolkit/

Project DeSHAME, available at https://www.childnet.com/our-projects/project-deshame/about-project-deshame

Helpful websites and materials for survivors and practitioners

https://www.endviolenceagainstwomen.org.uk

https://www.childnet.com

https://www.feministfrequency.com

https://feministinternet.com

https://fixtheglitch.org

https://gen-pol.org

https://www.hackharassment.com

https://www.lgfl.net/online-safety/default.aspx

https://securityinabox.org/en/

https://troll-busters.com/