unesco

Legal and Normative Frameworks for Combatting Online Violence Against Women Journalists

Angelique Lu, Julie Posetti and Nabeelah Shabbir

About this Publication:

This is an extracted chapter from a wider UNESCO-commissioned global study on online violence against women journalists produced by the International Center for Journalists (ICFJ). The full-length study was published in November 2022. This chapter critically analyses legal and normative responses to online violence against women journalists. It also provides action-oriented recommendations to help law enforcement agencies, the legal community and the judiciary respond more effectively to the crisis.

Over the course of the research period leading up to the full study's publication, and the publication of this extract, UNESCO and ICFJ have published a discussion paper, a report presenting the findings of the survey, and two individual chapters extracted from this study: What More Can News Organisations Do to Combat Gendered Online Violence? and Assessing Big Tech's Response to Online Violence Against Women Journalists.

CONTENT WARNING

This document includes graphic content that illustrates the severity of online violence against women journalists, including references to sexual violence and gendered profanities. This content is not included gratuitously. It is essential to enable the analysis of the types, methods and patterns of online violence. DISCLAIMER: The designations employed and the presentation of material throughout this publication do not imply the expression of any opinion whatsoever on the part of UNESCO concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views and opinions expressed in this document are those of the authors and should not be attributed to UNESCO.

Published November 2, 2022.

ICFJ ONLINE VIOLENCE PROJECT LEADERSHIP TEAM:

LEAD RESEARCHER/AUTHOR: Dr. Julie Posetti, Global Director of Research, International Center for Journalists (ICFJ); Senior Researcher, Centre for Freedom of the Media (CFOM), University of Sheffield; Research Associate, Reuters Institute for the Study of Journalism (RISJ), University of Oxford

SENIOR RESEARCHERS: Prof. Kalina Bontcheva (CFOM); Prof. Jackie Harrison (CFOM); Dr. Diana Maynard (CFOM); Nabeelah Shabbir, Senior Research Associate (ICFJ); Dr. Sara Torsner, University of Sheffield (CFOM)

RESEARCH ASSOCIATE: Nermine Aboulez, ICFJ researcher and University of Oregon PhD candidate

REGIONAL RESEARCH TEAMS:

AFRICA: Assoc. Prof. Glenda Daniels (Regional Lead); Fiona Chawana; Dr. Omega Douglas; Dr. Julie Posetti; Nabeelah Shabbir; Alexandra Willis

ARAB STATES: Nermine Aboulez (Regional Lead); Dr. Julie Posetti; Nabeelah Shabbir;

ASIA AND THE PACIFIC: Assoc. Prof. Fiona Martin (Regional Lead); Liana Barcia; Dr. Ayesha Jehangir; Nirasha Piyawadani; Dr. Julie Posetti; Dr. Jenna Price

CENTRAL AND EASTERN EUROPE: Dr. Greta Gober (Regional Lead); Jen Adams; Bojana Kostić; Nabeelah Shabbir

EUROPE AND NORTH AMERICA: Dr. Julie Posetti (Regional Lead); Dr. Greta Gober; Prof. Jackie Harrison; Nabeelah Shabbir; Dr. Sara Torsner; Prof. Silvio Waisbord

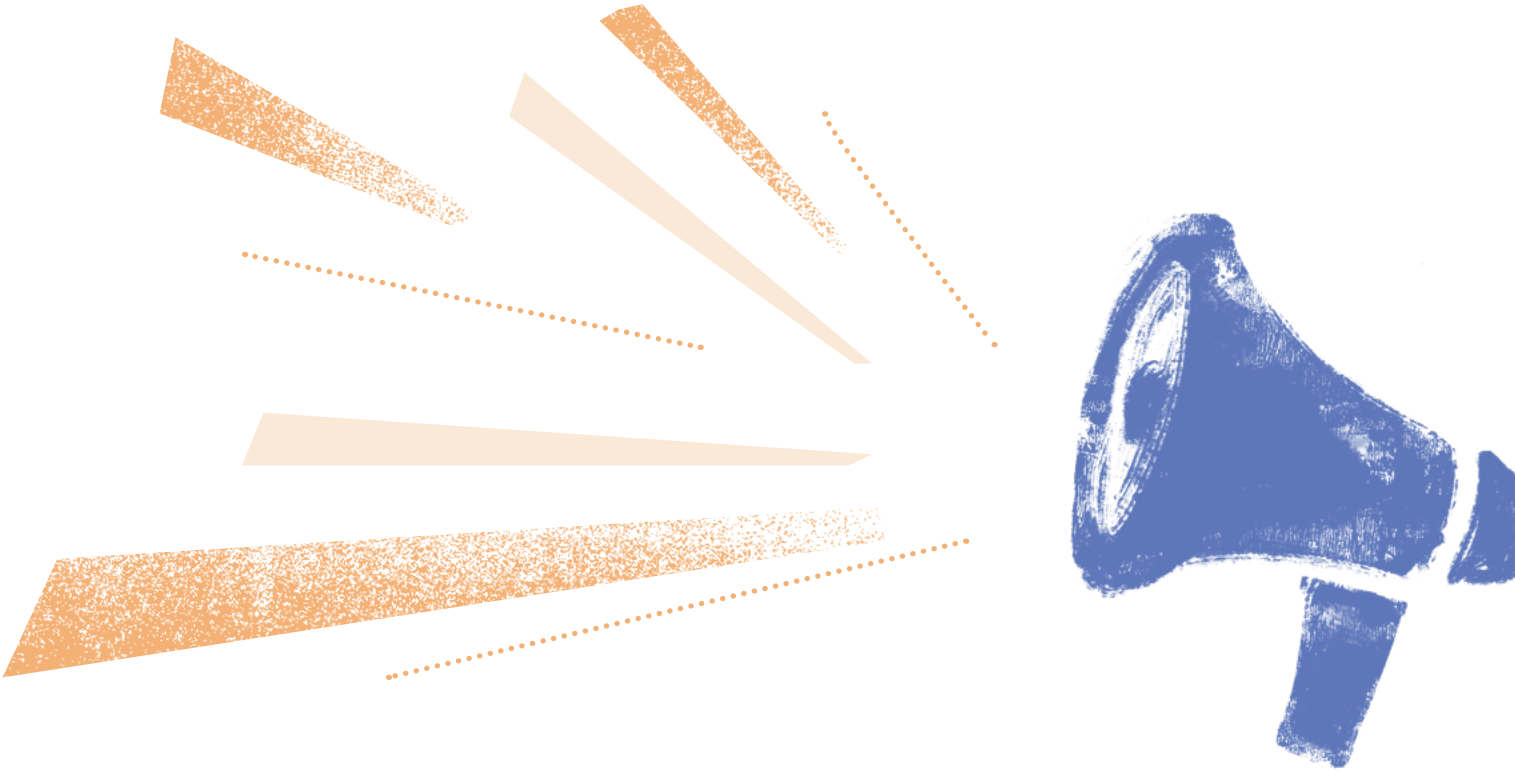
LATIN AMERICA: Dr. Luisa Ortiz Pérez and Dr. Yennue Zárate Valderrama (Regional Leads); Dr. Kate Kingsford; Carolina Oms; Dr. Julie Posetti; Nabeelah Shabbir; Kennia Velázquez; and Prof. Silvio Waisbord

SPECIALIST RESEARCHERS: Becky Gardiner and Angelique Lu

UNESCO COORDINATION: Saorla McCabe, Theresa Chorbacher, Guy Berger, and Guilherme Canela

PROJECT SUPPORT: Jen Adams; Fatima Bahja; Heloise Hakimi Le Grand; Mark A. Greenwood; Mora Devi S. Hav; Senka Korać; Juan Mayorga; Cristina Tardáguila; Eunice Remondini; Erin Stock; Joanna Wright; Mengyang Zheng (ICFJ/CFOM); Johann Bihr; Sara Bonyadi; Annina Claesson; Lou Palin; Dana Muresan; Antonia Eser-Ruperti (UNESCO)

ICFJ PROJECT PARTNERS: Centre for Freedom of the Media (CFOM), University of Sheffield; Dart Asia Pacific; Ethical Journalism Network (EJN); International Association of Women in Radio and Television (IAWRT). This project has received financial support from UNESCO's Multi-Donor Programme on Freedom of Expression and Safety of Journalists and the Swedish Postcode Foundation



The right to freedom of expression, with its corollaries of press freedom and freedom of access to information, is protected by Article 19(2) of the International Covenant on Civil and Political Rights (ICCPR) (OHCHR, 1976), and Article 19 of the Universal Declaration of Human Rights (UNDR) (UN, 1948). These articles require States to guarantee the right to seek, receive and disseminate information for citizens generally and, by extension, journalists and news publishers who benefit from press freedom protections. In 2011, the UN Human Rights Committee recognised that these rights also included "electronic and internet-based modes of expression" and called on Governments to protect any attack on an individual's right to their freedom of expression (OHCHR, 2011a). Since 2016, the UN has made it clear that "...the same rights that people have offline must also be protected online" (A/RES/71/199) (UN GA, 2016; UN GA, 2018b).

The UN Human Rights Council and the UN General Assembly have also recognised that women, and especially women journalists, are disproportionately affected by online violence, acknowledging that they are particularly exposed through intersectional factors such as race, ethnicity, sexual orientation and age (OHCHR, 2019; UN GA, 2017d; UN GA, 2017e; UN GA, 2018b; UN GA, 2020b; UN GA, 2021b).

In this chapter, international, regional and State-level legal and normative frameworks for responding to online violence against women journalists are examined, while exemplar judgements are catalogued, and gaps in law enforcement are highlighted. Here, insights gleaned from 184 in-depth interviews, and responses to the relevant survey questions in the main data corpus are supplemented by relevant examples from other countries, surfaced through extensive desk research.

Additionally, the 15 country case studies underpinning the broader study are drawn on to contextualise the discussion.

i. An assessment of relevant UN-level responses

a.The UN's specific measures to address the issue of violence against women journalists

The United Nations' legal and normative frameworks addressing violence against women journalists have grown and evolved over the decades. UNESCO, the UN organisation that commissioned this research, has a mandate to protect freedom of expression. It also plays a central role in the UN's work to improve the safety of women journalists, spearheading the implementation of the UN Plan of Action on the Safety of Journalists and the Issue of Impunity. The UN Plan of Action was developed in 2012 to coordinate the efforts of actors - both within and outside the UN system - in promoting a safer environment for journalists worldwide. In its 10th anniversary year, the Plan is under review to render it fit for purpose in the Digital Age.[1]

A 2016 Human Rights Council Resolution (33/2) on the Safety of Journalists specifies that States must prosecute attacks of all kinds, including gender-specific attacks, create protective measures for journalists, facilitate independent investigations, and ensure victims have access to appropriate remedies.[2] Additionally, the resolution explicitly refers to the specific threats faced by women journalists, and the need to take a 'gender-sensitive' approach when considering mechanisms to improve safety.

In 2017, the UN Secretary-General addressed the problem of online violence in his report to the UN General Assembly on 'The Safety of Journalists and the Issue of Impunity' (A 72/290). Shortly afterwards, the UN General Assembly adopted resolution (A/C.3/72/L.35/Rev.1) (UN GA, 2017e) on the safety of journalists with a particular gender focus, "condemning unequivocally" all "specific attacks on women journalists in the exercise of their work, including sexual and gender-based discrimination and violence, intimidation and harassment, online and offline."

The UN General Assembly passed another Resolution on the Safety of Journalists (A/RES/74/157) in 2019 that again condemned attacks on women journalists online and offline, including sexual harassment, intimidation and incitement to hatred. It also called upon States to "...tackle these issues as part of broader efforts to promote and protect the human rights of women, eliminate gender inequality and tackle gender-based stereotypes in society".

In 2020, the UN Special Rapporteur on violence against women, Dubravka Šimonović, submitted a thematic report on the issue of violence against female

1 See this 2022 report from the UN Special Rapporteur for the right to freedom of expression for an assessment of digital era gaps in the UN Plan of Action on the Safety of Journalists and the issue of impunity: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/323/44/PDF/G2232344.pdf?OpenElement=

2 "Resolution adopted by the Human Rights Council on 29 September 2016: the safety of journalists": https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/226/24/PDF/G1622624.pdf?OpenElement

journalists to the UN Human Rights Council (UN GA, 2020a). The report found that the rise of the internet also coincided with an increase in online attacks against women journalists, disproportionate to those faced by their male colleagues, as well as a rise in online violence such as doxxing, 'sextortion' and 'trolling'.

It also made a series of recommendations to States, including prohibiting and criminalising gender-based online violence against women journalists, creating investigative units or independent commissions to investigate these issues, as well as developing training protocols for law enforcement to better prosecute cases.

Also in 2020, the UN Human Rights Council passed a Resolution on the Safety of Journalists (A/HRC/45/L.42/Rev.1) which calls on States to:

> *… take measures to prevent sexual harassment and other forms of sexual and gender-based violence, including threats of rape, intimidation and harassment against women journalists, to encourage the reporting of harassment or violence by providing gender-sensitive investigative procedures…and to prohibit incitement to hatred against women journalists, online and offline, and other forms of abuse and harassment through relevant policy and legal measures that comply with international human rights law* (UN GA, 2020b).

Then, in mid-2021, the Human Rights Council passed a Resolution (UN GA, 2021b) that condemned unequivocally:

> *…online attacks against women and girls, including sexual and gender-based violence and abuse of women, in particular where women journalists, media workers, public officials or others engaging in public debate are targeted for their expression, and calls for gender-sensitive responses that take into account the particular forms of online discrimination.*

States, therefore, can be understood to have an obligation to prevent and stop online violence against women journalists, human rights defenders, and other public figures under their broader duty to protect freedom of expression (including press freedom), and end discrimination and violence against women and girls - online as well as offline.

However, States may limit or restrict freedom of expression if a three-part test is satisfied, in line with the provisions of Article 19 of the ICCPR, as explained in General Comment 34 (ARTICLE 19, 2020a):

- **The restrictions must be "provided by law": any restrictions on the right to freedom of expression must be explicitly drafted, to enable people to adjust their conduct appropriately;**
- **The restrictions must pursue a specific "legitimate aim": any restrictions must have the purpose of protecting the rights and reputations of others; and**

- **The restrictions must be "necessary and proportionate" to its intended goal.**

In this context, freedom of expression is not an absolute right. On the one hand, this means that freedom of speech defences cannot be used to justify abuses of the rights of others, and neither can they be used to fend off justifiable restrictions by a State acting within the international standards for legitimate limitations on expression.

Nor can 'freedom of speech' be used to excuse failing to act against online violence by those private actors whose facilities and platforms are exploited by attackers. The notion that a person's right to 'free speech' therefore entitles them to undercut another person's right to freedom of expression (including press freedom) is contrary to international standards on freedom of expression.[3]

On the other hand, as former UN Special Rapporteur for freedom of expression David Kaye warned in a 2017 report, any attempts by States to stop and prevent gendered online violence must also avoid censorship: "Censorship and undue restrictions on content could end up undermining the rights of the very women for whom governments and corporate actors may seek to provide redress" (OHCHR, 2017a).

In other words: at the UN level, countering online violence against women journalists while respecting freedom of expression is a 'balancing act' (Bontcheva and Posetti, 2020). But it would be a false binary argument to suggest that it is not possible to both defend freedom of expression while also working to prevent and stop online violence against women journalists - a form of attack which is ultimately designed to chill their reporting and undercut press freedom.[4]

b.UN-based frameworks to protect women and girls online

Women journalists experiencing online violence can also look to UN-level protections more broadly enshrining the rights of women and girls online and offline. Women's rights are protected generally under a number of other UN articles. For example, Article 2 of the International Covenant on Civil and Political Rights (ICCPR) requires states to guarantee human rights to all people "without distinction of any kind", including gender and sex. Further, the Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW) reates specific obligations to end discrimination based on gender and sex characteristics that would restrict a woman's human rights (UN Treaty Collection, 1979).

In 2013, the UN Commission on the Status of Women (CSW) called on States to develop mechanisms to combat violence against women online (UNCSW, 2013). The General Assembly went further later the same year, recognising that female human rights defenders were at risk of violence both online and offline by State and non-state actors, calling on States to bring perpetrators to justice (UN GA,

3 For a detailed discussion regarding the limits to freedom of expression, please see: https://unesdoc.unesco.org/ark:/48223/pf0000378755?posInSet=4&queryId=30ca5706-029b-4911-b525-e067c8e66a87

4 See the 25-point plan for States to respond to online violence against women journalists while respecting freedom of expression rights ina parallel chapter from this study, available here: https://www.unesco.org/en/safety-journalists/safety-women-journalists

2013). The Human Rights Council confirmed that domestic violence could include acts such as cyberbullying and cyberstalking in 2015 (OHCHR, 2015).

In 2017, the Special Rapporteur on Violence Against Women, Dubravka Šimonović, presented a report to the General Assembly, in which she suggested the formulation of a new legal framework for addressing violence against women (UN GA, 2017e). In the same year, the UN Committee for the Elimination of Discrimination Against Women (CEDAW) also recognised that gender-based violence occurs in technology-enabled settings (ARTICLE 19, 2020a).

The following year, the UN Human Rights Council (HRC) commissioned the aforementioned thematic report into gendered online violence (UNGA, 2018a). That report began by looking at legal issues linked to the terms "Information and Communications Technology (ICT)-facilitated violence against women" and "online violence against women" (ibid.). It defines the latter term as extending "to any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT…because she is a woman, or affects women disproportionately" (ibid.). The report concluded that the internet is being used in a broader environment of widespread and systemic structural discrimination and gender-based violence against women and girls, and it drew a number of other relevant conclusions:

- **International human rights law and other UN-related instruments pertaining to women in public and private life are fully applicable in digital spaces;**
- **Any legal and policy measures used to eradicate online gender-based violence should be framed within the broader framework of human rights (i.e. encompassing the right to freedom of expression);**
- **States should enact new laws and measures to prohibit new and emerging forms of online gender-based violence.**

Possible solutions proposed included:

- Increased education and training on the issue of online abuse and violence;
- Lobbying technology companies to develop mechanisms that allow individuals to control and define their online experience. These include tools that permit them to block specific individuals, control their privacy, or tailor their interaction to protect themselves against abusive behaviour;
- Increased funding for research into the scale of the issue (UN GA, 2018a).

Further, in 2018, the UN Human Rights Council adopted Resolution 38/5 on accelerating efforts to eliminate violence against women and girls in digital contexts (OHCHR, 2018c). The resolution acknowledged the effects of gender-based violence on the participation of women in the digital realm, and the obligations of States to prevent and protect such abuses from occurring, as well as highlighting the role that businesses need to play in addressing the issue.

In 2019, launching the UN Strategy and Plan of Action on Hate Speech (UN, 2019), Mr Guterres said: "Around the world, we see a groundswell of xenophobia, racism and intolerance, violent misogyny, antisemitism and anti-Muslim hatred" (UN News, 2019). The Plan acknowledges the exploitation of social media as platforms for bigotry, which see public discourse weaponised for political gain by stigmatising and dehumanising women and other targets such as minorities and refugees.

At a normative level, therefore, the UN has increasingly recognised the problem of online violence against women journalists, putting it forward as a matter of serious concern and calling for action in the international arena.

ii. Third party intermediary legal obligations

There are also a number of relevant human rights instruments relating to the human rights obligations of third-party platforms, such as Facebook, Google, TikTok and Twitter. Social media companies have an obligation to protect human rights as set out by the UN 'Ruggie' Guiding Principles on Business and Human Rights (OHCHR, 2011b).[5] These principles require companies to respect the rights established in core human rights treaties, including women's rights and the right to freedom of expression, press freedom and the safety of journalists. In particular, businesses must avoid violating human rights or facilitating human rights violations, and remedy them if they occur. They must also seek to prevent and mitigate any issues linked to their operations, products or services (ARTICLE 19, 2020a).

There is a question of the extent to which States have made internet companies legally liable for third party content that violates human rights. Given the debate and the diversity of jurisdictions on this issue, a number of different approaches have also been developed. In the US, where there is no legal liability for third party content, the Federal Trade Commission fined Facebook $5billion for consumer privacy breaches in 2019 (FTC, 2019). In France, Reporters Without Borders (RSF) instigated a consumer law case against Facebook in March 2021. RSF alleges that Facebook is guilty of "deceptive commercial practices" on the grounds that the company's promises to provide a "safe" and "error-free" online environment are "largely mendacious", and "that it allows disinformation and hate speech to flourish on its network (hatred in general, and hatred against journalists), contrary to the claims made in its terms of service and through its ads" (RSF, 2021p).

iii. Regional legal frameworks and instruments

Various regional bodies have recognised the generic need for protection of human rights on the internet companies' services. For example, in 2013, the Special Rapporteur for Freedom of Expression of the Inter-American Commission on

5 See also Chapter 5.0, "Platforms and vectors: Assessing big tech responses to online violence".

Human Rights (IACHR) recommended that private actors establish services that are consistent with human rights laws (Botero Marino, 2013).

Other recommendations included the publication of transparency reports about government requests for user data or content removal. It was also recommended that efforts be made to notify individuals who may have their rights violated, granting them access to non-judicial remedies and creating protective measures and business practices consistent with human rights protections (ARTICLE 19, 2020b).

Similar recommendations were made by the subsequent IACHR Special Rapporteur in 2017 in his report 'Standards for a Free, Open and Inclusive Internet,' which noted "the relevant policies and practices must be based on respecting and guaranteeing human rights" (Lanza, 2017).

Towards the end of 2021, the Inter-American Court of Human Rights found the State of Colombia responsible for the kidnapping, torture and rape of El Espectador journalist and former UNESCO World Press Freedom Prize winner Jineth Bedoya Lima by far-right militia (AFP, 2021), in a judgement which referenced research for this study to highlight the online-offline nexus (IACHR, 2021b).

The specific need to recognise and address gendered online violence against women journalists has also been examined by regional bodies such as the Organization for Security and Cooperation in Europe (OSCE), the Council of Europe (CoE), the European Court of Human Rights, the European Commission and the IACHR. Each of these has explored similar themes about the safety of women journalists (ARTICLE 19, 2020a).

Article 17 of the Council of Europe Convention on preventing and combatting violence against women and domestic violence (Istanbul Convention) requires Member States to actively encourage the private sector and the news media to help prevent violence against women (Council of Europe, 2011). In 2016, the Council of Europe adopted a recommendation on the safety of journalists, which recognised that women journalists faced gender-specific threats which were increasingly taking place online. The guidelines called on States to "take appropriate preventive operational measures'', such as police protection, taking into account "gender-specific dangers" (Council of Europe, 2016).

The Organization for Security and Cooperation in Europe (OSCE) has also been significantly involved in developing norms to protect women journalists from online violence. In 2016, the OSCE Representative on Freedom of the Media recommended that States recognise threats and harassment of female journalists as an attack on freedom of expression as part of its Safety of Female Journalists Online project (OSCE, 2016b). The report suggested a number of mechanisms to address the issue, including the improved training and strengthened capacity of law enforcement, as well as the collection of data to determine the extent of the issue. OSCE's work on this issue continues, with a 2020 study making a series of concrete and tailored recommendations for action, including within legal and judicial arenas, directed at both State and non-State actors (Chocarro et al., 2020).

The nature of the internet means that any person across the world can engage in online violence. However, in the landmark 'right to be forgotten' case against Google, the Court of Justice of the European Union, found that Google was bound

by EU laws. The court ruled that even if physical servers were outside of the EU, laws applied to search engine operators if they have branches in a Member State (EUR-LEX, 2014).

In late 2021, the European Parliament voted in favour of stronger regulatory responses to the problem of harms such as online violence and the spread of disinformation as part of the proposed Digital Services Act (DSA) which focuses on content moderation and aims to "create a safer digital space in which the fundamental rights of all users of digital services are protected" (European Commission, 2021a). It is "building a new framework, so that what is illegal offline is also illegal online" (European Parliament, 2021). The potential extra-EU dimensions of this initiative will become evident over time.

Under Articles Two and Three of the Council of Europe's European Convention on Human Rights, there is an obligation to conduct an investigation when there is a death of a journalist which may implicate a government, or where the State may have had a protective obligation with which it failed to comply. Article Three - the right to freedom from inhuman and degrading treatment - could also extend to many acts of gender-based online violence. However, this concept is not yet well developed at the international level.

iv. Practical legal challenges experienced by women journalists under fire

Traditional legal routes are often costly, emotionally taxing, convoluted and ill-equipped to provide adequate redress for the targets of gender-based online violence. Tort law-based suits[6] could potentially provide some form of remedy for victims, however there are limitations. Legal routes such as privacy torts, copyright, or even laws that were written for analogue communications methods like telephone and mail are being tested, but they are often deemed to be unfit for purpose in regard to online violence against women journalists, both domestically and across jurisdictions.

Tort actions require being able to identify perpetrators, while laws criminalising harassment and stalking usually require proximity and repetition - making legal remedy in a case involving a 'pile on' instigated by a perpetrator who posts a one-off threatening comment from the other side of the world very challenging. Such laws are also often interpreted as applying only to the physical realm.

The jurisdictional issues that exist in criminal law are also found in civil actions. Secondly, civil law proceedings may bring more attention to a matter, which can deter complainants. Thirdly, a victim may not be seeking an award of damages, but rather an injunction to remove content or de-platform a perpetrator, meaning that conventional remedies in civil law may not be appropriate. Finally, civil law remedies may only be used after the event has occurred: they cannot prevent the publication of abusive, threatening or harassing content at the outset, limiting their role as preventive measures, although successful prosecutions and verdicts may be effective deterrents in some arenas.

6 Tort law is the branch of law that imposes civil liability for breach of obligations imposed by law e.g. negligence cases. See: https://uk.practicallaw.thomson-reuters.com/6-107-7397?transitionType=Default&contextData=(sc.Default)&firstPage=true

Research conducted for this study identified the following **12 legal, judicial and law enforcement factors presenting challenges to, and potential opportunities for, legal remedy.**

1. Platform accountability

The internet services that primarily enable online violence are legally protected from liability for content in most instances, providing very little incentive for them to police the behaviour of users or recalibrate their algorithms in ways that prioritise human rights over profit. Nevertheless, companies like Facebook, Google and Twitter have come under increasing pressure over their role in facilitating and enabling the online harassment and abuse of women journalists. However, due to being based in the US, these companies are currently shielded by Section 230 of the Communications Decency Act (CDA) which generally protects them from liability for the speech of others published on their platforms, even if said speech is found to be illegal (Lipton, 2011).

Section 230 protects companies from tortious actions involving their users. It was passed in 1996, and has been lauded as "the most important law protecting internet speech" (Harvard Law Review, 2018). Some commentators credit this law for allowing the internet to thrive. However, many researchers have noted that the law was introduced before the advent of the social web, and it actively prevents victims of gendered online violence from pursuing legal action against the internet companies for the actions of their users.

In 2015, journalist Alex Chu wrote a public appeal to the then US President Barack Obama to repeal Section 230. It continues to resonate:

> *Right now you can't sue digital platforms for enabling harassment on their services, even if they enable harassment through flagrant, wilful neglect. If your harasser is able to take fairly basic steps to keep himself anonymous — and if the platform he chooses enables and enforces that anonymity — then there is literally nothing you or the government can do, even if his actions rise to the level of major crimes like attempted murder. Closing this loophole wouldn't require giving the internet "special treatment" compared to other forms of communication. Nor would it require a sudden, major deviation from the standards of free speech most of the developed world respects. It would require the exact opposite — it would require the United States to remove a law that specifically mandates special treatment for internet service providers and platforms that no other communications medium has...* (Chu, 2015).

Some scholars have suggested including a take-down provision in the CDA, similar to the safe harbour provision found in Section 12 of the Digital Millennium Copyright Act (DMCA), which protects services that inadvertently host material that infringes copyright (MacAllister, 2017). More recently, whistleblowers exposing Facebook's failure to deal with predictable harms on its platforms have also

called for reforms to the CDA (see discussion below). In a 2021 report, the Aspen Institute's Commission on Information Disorder also recommended that Section 230 be amended to a) Withdraw platform immunity for content that is promoted through paid advertising and post promotion, and b) Remove immunity as it relates to the implementation of company product features, recommendation engines and design (Aspen Digital, 2021).

However, ARTICLE 19's Legal and Policy Officer Paulina Gutiérrez expressed concern about subjecting the platforms to regulatory systems governing news media as a means of achieving improved responses to online violence. She argued that as internet intermediaries, they should not be regarded as news publishers held responsible for third party content on their sites and apps: "This is a very important freedom of expression principle that we need to uphold even in these cases. We need to start looking at other regulatory models, like what can we ask [of] them that is free speech compliant; privacy compliant". But this view runs counter to that expressed by many international editors and journalists interviewed, who generally argued in favour of the platforms being legally required to fulfil the same obligations met by publishers.

Blowing the whistle

Whistleblowers exposing Facebook's failure to deal with predictable harms on its platforms have also increasingly called for reforms to the CDA. As mentioned above, in October 2021, former Facebook product manager Frances Haugen disclosed a cache of internal company documents and urged the US Congress to amend Section 230 with the aim of regulating companies to redesign algorithms that emphasise engagement and inflame hate, as distinct from their liability over user-generated content.

In late 2021, Facebook shareholders resolved to commission an independent human rights impact assessment on the targeted advertising systems that drive the company's profits. The resolution cited data from Ranking Digital Rights' Index on the company's lack of transparency around how it enforces its advertising policies (Investor Alliance for Human Rights, 2021). Facebook derives 99% of its revenue from advertising, but the company publishes nothing about how many ads it takes down, how effectively it detects (and deters) bad actors, and how often its various ad rules are broken. "Facebook continues to evade transparency on this topic while making every effort to block independent research that aims to unearth more information on how it enforces its rules", tweeted Ranking Digital Rights (RDR, 2021).

Time for news organisations to take legal action against the platforms?

Several of our interviewees expressed scepticism about the prospect of regulatory reform making the platforms accountable for online violence against women journalists, including Inga Thordar, a senior editor at CNN at the time of her interview. She suggested that a class action lawsuit brought by major international news organisations might be a more effective approach.

Kenyan editor Catherine Gicheru of the Africa Women Journalism Project told the researchers:

> *We need to start taking people to court for their online behaviour because it is affecting our capacity to report freely as female journalists, impeding our right to free expression… The media should test the laws that exist and take these perpetrators to court. I know that many of these cases may be dismissed, but it is an excellent starting point for engaging the police and government to enact or strengthen current anti-harassment laws to recognise harassment in online spaces. As it is, if you report online harassment to the police today, they are frequently at a loss as to how to document your complaint unless you can provide them with physical evidence of the harassment.*

Such legal action is not easy, as demonstrated by Sweden's Cyber Hate Crime Monitor, which pursued domestic legal action to get Facebook to take responsibility for toxic content in closed and 'secret' Facebook groups in 2019. The organisation documented 80 clear examples of criminal statements published within one such group. They submitted a 'legal removal request', with 80 statements attached, asking Facebook to close down the group, or alternatively that the company moderate the group - but Facebook rejected the application. Instead, the company suggested that the Cyber Hate Crime Monitor should go through the various groups identified and report each criminal activity spotted. The organisation then reported Facebook to the police for violating the act on responsibility for electronic bulletin boards, but they did not proceed with an investigation. The Cyber Hate Crime Monitor continues to pursue legal action against Facebook in the case (Cyber Hate Crime Monitor, 2020a; Cyber Hate Crime Monitor, 2020b; Swedish Television, 2020).

2. Identifying the perpetrators

At the individual State level, conventional legal remedies (including law enforcement tools like protective orders) are often dependent on being able to identify the perpetrator, which is difficult when anonymous usernames and VPN devices are designed to prevent identification. When perpetrators are unfamiliar to the victim, or go to great lengths to conceal their identity, significant resources are required to investigate, locate and identify harassers (Fenwick, 2021). Police and law enforcement officials may also have to rely on the cooperation of the platforms to carry out their investigations, which can often be time-consuming, and may not lead to successful identification of perpetrators. These factors may reduce the likelihood of a successful prosecution, which could deter prosecutors from taking on cases involving the harassment of women journalists.

Some proposed legislative responses involve 'real-naming conventions' for social media users to enable easier identification of perpetrators. This raises privacy issues,

however, and also could weaken the important function of source confidentiality and anonymity in investigative journalism (Posetti, 2017a). One example of this approach is the Australian legislative push of late 2021 designed to require social media companies to supply details of users who defame or harass others. It will incorporate a complaints mechanism with takedown enforcement powers. "They have created the space and they need to make it safe, and if they won't, we will make them (through) laws such as this," the Australian Prime Minister said (Reuters, 2021c). The proposed legislation comes in response to a ruling by the country's High Court which held news organisations, not Facebook, liable for defamatory third party comments made on a news publisher's post. It also follows defamation action by a senior cabinet minister against a human rights defender over a critical tweet focused on the minister's public statements regarding a high profile rape case (Karp and Remeikis, 2021).

3. Cross-jurisdictional challenges

Jurisdictional issues remain one of the biggest challenges in combating gendered online violence. For example, UK based human rights lawyer Caoilfhionn Gallagher QC said in an interview that the Council of Europe mechanisms are generally only effective when dealing with Council of Europe Member States. So, when non-Member States are associated with attacks on journalists in Europe - online or offline - there is very little that can be done to hold them to account.

One significant case carried by Gallagher involves online violence being experienced by women journalists at the BBC Persian language service.[7] They are UK residents who are being targeted in an orchestrated online violence campaign that they believe is emanating from Iran, a non-EU Member State, and removing such content from view online only within Europe would have limited effect.

Successful prosecution of gender-based online violence requires cooperation between the platforms, law enforcement agencies, and often multiple jurisdictions (across countries or federal states), which may pose significant challenges. Even if perpetrators can be identified and located, assuming devices like VPNs are not used to hide their IP addresses, they could be inaccessible due to jurisdictional issues which dramatically reduce the likelihood of a successful prosecution against individuals, or US-based social media companies.

Law enforcement across international borders may depend on mutual legal assistance treaties (MLATs) to gain access to evidence and to identify perpetrators through international cooperation (ARTICLE 19, 2020a). Although research shows they are a 'resilient' form of obtaining data, they are rarely used by law enforcement agencies. MLATs can take months, are often costly, require complex administrative legal processes, and the cooperation of other countries and third-party platforms. Civil society organisations have also raised concerns about possible privacy violations and a lack of transparency about their application (ibid).

7 See Chapter 2, "Global Overview: comparative analysis of incidence, impacts and trends" and Chapter 5.3, "Policy gaps" of the full study [https://www.icfj.org/our-work/icfj-unesco-global-study-online-violence-against-women-journalists] for more about BBC the case involving Persian journalists.

The case of Qatar-based journalist Ghada Oueiss[8] is relevant to jurisdictional limitations. She is taking legal action in a US court against residents of two other States, the UAE and Saudi Arabia, in connection with what she alleges is an example of orchestrated online violence by foreign political actors and their agents. The action is being pursued in a Florida court and it names various State actors, State media, and US-based social media users (Shilad, 2021a).[9]

One Twitter account targeting Oueiss grew to 50,000 followers in three weeks, prompting her to take legal action. "I had no choice but to file the lawsuit. That was the only way to respond, because it was becoming more and more vicious," she said. However, the case and others like it, face major technical hurdles, including jurisdictional issues (Clary, 2021).

These cases raise the issue of international legal processes dealing with cross-border harm. For example, in response to the murder of US-resident Jamal Khashoggi in Saudi Arabia's Istanbul Consulate, Reporters Without Borders (RSF) applied to the German courts for remedy for 'crimes against humanity' under the German Code of Crimes against International law (VStGB). German laws offer jurisdiction over core international crimes committed overseas, and "German courts have already shown readiness and willingness to prosecute international criminals" (RSF, 2021p).

Inconsistent laws within a country can also make the prosecution of online violence against women journalists more difficult. For example, all US states criminalise the stalking or harassment of a person, but inconsistent laws relating to the internet have been highlighted as a key impediment to developing a national approach to the problem. Some legal researchers argue that the existing framework of disjointed laws in the US is ill-equipped to deter conduct that crosses state and national borders (Lipton, 2011).

One possible approach is to draft legislation so that any legal actions are based on the jurisdiction where the victim lives, rather than the perpetrator.[10]

4. Criminal Remedies for Harassment, Stalking and Threats

Laws covering online violence are also often drawn from offline stalking and harassment legislation. This may be problematic, given many harassment laws were drafted before the advent of the internet and may not be fit for purpose. Additionally, the internet arguably makes harassment easier to execute, enables it to attain virality, and can elevate physical risk. A complicating factor involved with laws covering stalking offences is the need for 'repeated' communications. This element of the law, examined in reference to online 'pile-ons', means that someone who posts a threat on a single occasion may not be covered by the provision.

8 See case study in Chapter 2.2.1: "Racial vilification and structural racism".

9 Ghada Oueiss' original court filing: https://www.courthousenews.com/wp-content/uploads/2020/12/1-20cv25022-002.pdf

10 See for example: Dow Jones & Company Inc. v Gutnick, Joseph (2002) HCA 56 which held that defamation occurs where the loss to reputation occurs (High Court of Australia, 2002).

In Ireland, a man was sentenced to four and a half years in prison in 2018 for harassing RTÉ journalist and presenter Sharon Ní Bheoláin. The case involved an early example of a harasser producing what are now known as deepfakes. The man uploaded 32 pictures to a website which had been doctored to show Ní Bheoláin's head on pornographic images which could be searched for online. The site was shut down during the police investigation. The officers also uncovered private messages in which he named Ní Bheoláin while discussing torture, murder and extreme sexual violence (McCully, 2019). When sentencing the man, the judge described his actions as an "insidious form of harassment" and "debasing behaviour", noting that the "information on [Ms. Ní Bheoláin] will be out there forever" and "no doubt it caused considerable distress... It was reprehensible and he should be thoroughly ashamed" (INSI, UNESCO and TRF, 2021). The following year (2019), another man, a self-described "internet troll" was sentenced to five years in jail after targeting six Irish women journalists with hundreds of abusive emails. While noting the internet's "wonderful advantages", the judge said it also had a "dark side which allows a man sitting in his house to inflict huge amounts of trauma on six women" (ibid).

New Irish legislation from February 2021 - Harassment, Harmful Communications and Related Offences Act 2020, known as the 2020 Act - specifically includes online harassment and cyberstalking; whilst Section 10 of the Non-Fatal Offences Against the Person Act 1997 (the 1997 Act) is the primary legislative provision in Ireland for the prosecution of incidents of harassment (INSI et al., 2021). Under Irish law, it would need to be established that a perpetrator intended for the threat to be believed, and there would have to be persistent abuse to prosecute cases of online harassment which did not include threats to kill or cause serious harm (ibid.).

In France, in 2018, radio journalist Nadia Daam became the target of online violence (considered a form of moral harassment under French law) after she criticised the actions of members of an online forum during a broadcast. Her employer, Europe 1, filed a complaint on her behalf to the police, who then identified seven possible perpetrators, leading to two people being brought before the court.

The charges concerned a rape and death threat which superimposed Daam's face onto an image of a victim of the so-called Islamic State. Both men were given six-month suspended prison sentences and were fined 2,000 Euros (McCully, 2019). The Paris Court of Appeal ruled that the incriminating messages were "intended to 'punish' Daam as a journalist" covering women's rights, and "deserved a sentence sufficiently dissuasive to prevent a new offence, particularly via the internet, a communication tool perfectly mastered by the accused who, acting under a pseudonym, which proves his cowardice, could only be identified thanks to the cyber investigations of the police" (INSI et al., 2021). This case was successfully prosecuted under Article 222-17 of the French Penal Code, which criminalises threats to commit a crime. However the Article has a high evidentiary burden, with the prosecution needing to demonstrate a person making a threat knew and intended to create fear in the victim.

In the UK, two men were jailed in 2020 and 2021 for attacking journalist Amy Fenton[11] on Facebook in two separate episodes (Sharman, 2020; Tobitt, 2021a).

11 As noted in Chapter 2.5.5 of the full study (available here: https://www.icfj.org/our-work/icfj-unesco-global-study-online-violence-against-women-journalists) "Increasing offline security in response to online attacks",Amy Fenton, former chief reporter for The Mail in the north of England, has been subjected to extreme online violence with offline impacts in connection with her

In the first instance, the man posted on her newspaper's Facebook page that she "needed raping". He was sentenced to five months in jail (Tobitt, 2020; 2020c). In the second case, the man sent Fenton Facebook messages threatening to shoot her. He was jailed for nearly six months for "sending by public communication [Facebook] an offensive, indecent, obscene or menacing message" (Tobitt, 2021). The court also issued restraining orders against the perpetrators in both cases.

In another UK case, in March 2021 a court issued a temporary stalking prevention order against a far-right figure to protect the Independent's Home Affairs correspondent Lizzy Dearden and her partner. It was alleged that the man threatened and harassed both Dearden and her partner online and offline, including at their home, in a bid to chill her reporting. The order prevented the man from contacting the couple, or publishing anything about them on social media unless referring to Dearden as the author when responding to any story written by her. Issuing the order, the Deputy Chief Magistrate said: "What the police say in this case is he has embarked on all of this to persuade her not to publish the story" (PA Media, 2021).

In Finland in 2018, three people were convicted of "stalking", in relation to coordinated attacks on investigative journalist Jessikka Aro. She was the subject of a four-year harassment campaign, after she published stories about foreign State-aligned troll factories (McCully, 2019). Aro filed a complaint with the police in Helsinki in 2016, and three people were ultimately prosecuted under three sections of the country's criminal law, with nine other people listed in the prosecution case as victims of the harassment campaign.[12] The Helsinki District Court held that the defendants had violated the country's criminal code by repeatedly contacting Aro by "tagging" her in social media posts, in a way that fit the legal definition of "stalking", among other factors (see discussion about the function of defamation law in this case below). One of the defendants was sentenced to 22 months in jail, while the other two received suspended jail sentences. The criminal code -which covers the offences of stalking prosecuted in this case - requires "contact", which could imply that only direct communications with a victim (i.e. DMs or posts in which they are tagged), and not messages to third parties about the target, or posts that make only oblique references to the victim, would be covered. The case also highlighted the issue that prosecutors are unable to launch proceedings without a complaint from a victim. Complaints forwarded by third parties, such as colleagues, employers, family members or bystanders are unable to compel a prosecutor to investigate unless the victim complains.

Difficulties defining online harassment

The absence of clear legal definitions as to exactly what behaviour constitutes actionable digital stalking, harassment or threats is one of the key legal issues affecting the prosecution of online violence against women journalists (ARTICLE 19, 2020a). Even when there is consensus that criminal sanctions should be applied, there are also issues about how the crime should be defined and when the threshold for criminal liability should be reached. Courts have struggled to

reporting on grooming gangs. She has reported more than 100 such threats to law enforcement (Pidd, 2020).

12 This case has some similarities with cases explored in this research, including Maria Ressa (the Philippines), Carole Cadwalladr (UK), Ghada Oueiss (Lebanon), Karima Brown (South Africa), and the BBC Persian language service group of journalists.

determine the nature of online threats, or provide guidance on which comments or content are worth prosecuting. One problem is the view that if online violence has not manifested offline, it is not sufficiently serious. There is also the problem of misogynistic speech being protected by free speech laws in the many countries where misogyny is not considered a hate crime, for example.

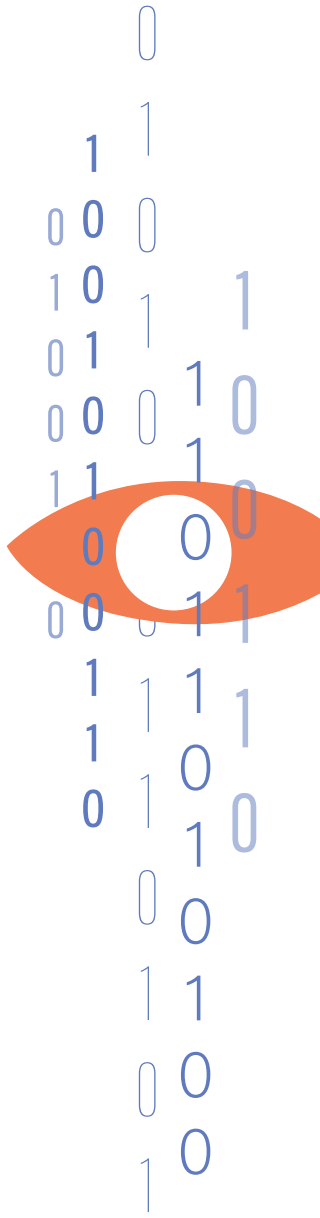
In 2014, a Swedish journalist reported a series of threats she received to the police. However, the court found that the following threatening statement was protected by freedom of speech provisions, due to its general nature: "To me gender equality is when you take a sexist feminist whore in the vagina with a large knife" (Edström, 2016). The court also ruled that it would not be acceptable to explicitly name the woman. Feminist legal scholars in the country argued that the court was enabling perpetrators to threaten women in a more generic way: "Those who hate adapt. Now they know they should not put the name of the person they are threatening in the postings" (ibid.)

In December 2020, the Lebanese parliament passed a law that criminalises sexual harassment. The penalties include up to two years in prison and a fine of up to 20 times the value of the minimum wage, 675,000 Lebanese pounds (Al-Arabiya News, 2020). The penalties can be increased to a four-year prison sentence and a fine of 50 times the minimum wage if the crime is more 'serious' (such as related to a work relationship). The law defines sexual harassment as "any bad and repetitive behaviour that is extraordinary, unwelcome by the victim, and with sexual connotation that constitutes a violation of the body, privacy, or emotions". Sexual harassment can take the form of offline and online speech and actions. It can also be a single or repeated occurrence that enforces psychological, moral, financial or racist pressures to obtain sexual benefits (Human Rights Watch, 2021a).

The Lebanese legislation states that sexual harassment cases need to be tried in a criminal court instead of a civil court. Advocates have criticised this requirement, suggesting that victims would be less likely to report incidents as a result (Human Rights Watch, 2021a; Al-Arabiya News, 2020). However, these concerns may be resolved if criminal proceedings were held in camera, or in private, in an attempt to protect would-be complainants, a process common in other international jurisdictions (Mhaidly, 2018).

Section 24 of Nigeria's 2015 Cybercrime Act penalises 'cyberstalking' or messages that are "false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will, or needless anxiety to another". In theory, this could be viewed as a legal mechanism that could be used by women journalists experiencing online harassment. However, civil society organisations say this law has been used to prosecute journalists, bloggers and activists (Freedom House, 2019; CPJ, 2018; CPJ, 2019b; CPJ, 2022).

One journalist was charged with four violations of the 2015 Cybercrime Act, from Sections 24 and 27: cyberstalking, sending defamatory messages using a computer, using a computer to send messages "for the purpose of causing public hatred", and using a computer to "bully, threaten and harass". He told advocacy groups he believed the charges were in response to his critical reporting ahead of an upcoming election (ibid). This highlights the potential for anti-online violence laws to be used to chill freedo of expression.



In Serbia, sexual harassment is reported to take place online at rates above average for the region (OSCE, 2019). The Criminal Code of Serbia was amended to add the crime of sex-based harassment (Article 182a) and stalking (Article 138a) in June 2017, with penalties including a fine and imprisonment of up to six months. The Code defines sex-based harassment as any "verbal, non-verbal or physical conduct that aims to violate the dignity of the person in the sexual sphere, which causes fear or creates hostile, degrading or abusive environment" (AWC, 2019).

Legal experts interviewed for this study emphasised that the Serbian courts might see online threats as lacking "the character to induce a sense of endangerment" (especially in cases where they come from powerful figures). Other criminal offences have been identified by the Standing Working Group for Journalists' Safety as applicable to online harassment of women journalists in Serbia, and are part of the Group's initiative for amending the Criminal Code. These include 'computer sabotage' (Article 299) and unauthorised access to computers, computer networks or electronic data processing (Article 302); and racial and other discrimination (Article 387 para. 2, 4 and 6) (Babović and Reljanović, 2018). Online attacks are investigated and processed through special departments such as the Special Prosecution for High Tech Crime in the Higher Public Prosecutor's Office in Belgrade, and under the scope of the Ministry of Interior's Special Department for Combating Cybercrime, established under the Law on Organisation and Competences of Government Authorities in the Fight against High-Tech Crime.

In 2018, Serbian journalist Verica Marinčić filed criminal charges against a man who was allegedly threatening her online and physically stalking her in connection with a news story (Djurić, 2019; Mapping Media Freedom, 2018; Apro, 2020). The accused man reportedly swerved his motorbike into her after she commenced legal action (Stojanovski, 2019). When she lost the case, she said: "I cannot report cases of harassment and intimidation anymore while I see how they are turning a victim into a fool" (Apro, 2020). According to the Slavko Ćuruvija Foundation[13] and the Centre for Judicial Research (CEPRIS), 70% of cases of reported attacks against journalists and media workers in Serbia end with the prosecution rejecting criminal charges. Nevertheless, Ana Lalić, journalist at Nova.rs, a Serbian news website, had six lawsuits in motion at the time of writing, all to do with instances of online violence. "I am fighting here for my name and for my personal integrity, which they are trying to tarnish," she said.

Some sections of the Sri Lankan Penal Code could be used to prosecute acts of cyber violence including sexual harassment, criminal intimidation, criminal breach of trust, blackmail, extortion, and impersonation. However, a fundamental problem is that women have described great difficulty reporting violence to the authorities in general: "With this legislation in place, it should theoretically be easy for victims to access justice for crimes committed against them online. However, most victims do not pursue these solutions due to flaws that exist in the system of reporting online violence to authorities" (Perera and Wickrematunge, 2019).

An anonymous Sri Lankan interviewee catalogued the problems she experienced in pursuit of justice as: a lack of specific laws to deal with gendered online abuse

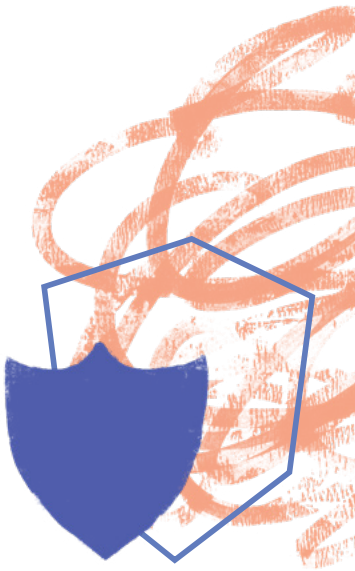
13 Civil society organisation founded in memory of the murdered Serbian journalist, which works to advance media freedom, and member of the Standing Working Group of Journalists.

and harassment; the absence of a designated law enforcement authority to handle complaints; a lack of knowledge of these crimes within the police force; and a lack of legal support to prosecute cases. She also argued that there needed to be more effective ways of reporting, documenting and investigating such crimes, including a hotline for complaints or a database for indexing and searching cases.

A 2020 report commissioned by the Media Council of Kenya found low levels of reporting of abuse to the police and poor follow-through by them. One reason may be the lack of knowledge among police officers about social media platforms and online violence, as suggested by interviewees for this study. Law enforcement may diminish or normalise the experiences of online violence and not see it as an urgent threat when no physical violence has yet taken place, according to interviewees.

But freedom of expression concerns have also been raised in Kenya, about the Computer Misuse and Cybercrimes Act proposed to regulate against the use and abuse of digital technologies which could cause harm or any form of criminal behaviour (Nitsche, 2019). The Act also sets out provisions to protect Kenyans or anyone living in Kenya against 'false publications', circulation of 'false information' and cyber harassment, with guidelines on protecting all citizens against crime, child pornography and false information (Articles 22, 23 and 27).

5. Defamation action as a defence



Defamation is a remedy found in common law jurisdictions to protect individuals against the publication of false statements about them that harm their reputation (Harvard Law Review, 2018).[14] Defamation and libel are key features of online violence against women journalists - especially in cases where disinformation tactics are deployed. However, there is a tension involved for many journalists here. This tension is based on the professional norm that journalists should not sue for defamation because defamation law is frequently used as a tool to suppress critical reporting, chill press freedom and limit the public's right to access information. However, freedom of expression protections do not extend to hate speech or disinformation which could damage someone's reputation, or intimidate them into discontinuing their reporting. Therefore, defamation, after due process of law, where the three-part test is applied,[15] could prove to be one of the more effective responses to online violence against women journalists.

In Finland, three people were convicted of "aggravated defamation" and "incitement to commit aggravated defamation" in 2018 in relation to the aforementioned coordinated attacks on investigative journalist Jessikka Aro. One defendant was the editor-in-chief of a website that published sexist abuse and racial slurs. In addition to criminal convictions for stalking (see point 4. above), the Helsinki District Court found that the defendants had:

- Published a series of false and defamatory articles about Aro;
- Encouraged others to publish defamatory statements about Aro;
- Committed copyright violations.

14 As long as they are applied in line with General Comment #34: https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

15 For more information on "The Legitimate Limits to Freedom of Expression: the Three-Part Test", see: https://www.youtube.com/watch?v=Wg8fVtHPDag

The three defendants in the case were convicted and ordered to pay a total of EUR €238,625 in damages, costs, and legal fees, and Aro herself received EUR €94,000 in damages.

Brazilian journalist Patricia Campos Mello won two relevant defamation actions in early 2021. She successfully sued powerful political figures for defaming her in connection with an onslaught of online harassment and abuse that followed her reporting on disinformation associated with Brazil's 2018 election. The judge ordered her attacker to pay Campos Mello US $5,500, saying that he "should have more caution with his statements — something that is expected from all those with some sense of responsibility to the nation" (Neder, 2021). In March 2021, Campos Mello also won her case against another attacker, who was ordered to pay her damages. According to the judge, the attacker's remarks had damaged her honour (BBC News, 2021b). Despite national and international attention and her court victories, online attacks against Campos Mello nevertheless continued on social media in mid-2021, highlighting the need for further preventive legal measures, and a stronger response from the social media companies serving as vectors.

Pakistan introduced the Prevention of Electronic Crimes Act (PECA) in 2016 with the stated objective of contending with online hate speech, extremist content and harassment against women. However, the legislation was criticised by human rights groups which argued that it could lead to the violation of freedom of expression rights and enable censorship. The law, administered by the Federal Investigation Agency (FIA), is perceived by some as a tool that can enable harassment of women, according to Human Rights Watch (Gossman, 2020). Nine complainants were charged with criminal defamation in 2020 under Section 20 of PECA, while many complaints about online violence against women journalists have remained unaddressed (ibid).

6. Privacy-based legal action

Gender-based online violence against journalists often violates the privacy of victims, and there may be legal avenues found in privacy laws. In Scotland (United Kingdom), for example, a person can be sued for 'breach of confidence' which seeks to protect violations of a victim's 'autonomy, dignity and self-esteem' (Hill, 2015). Under the tort, the court would consider whether the subject had a reasonable expectation that content (e.g. intimate images) would remain private. It is arguable that this could allow women to sue for so-called 'revenge porn' forms of gendered harassment. However, suing for privacy breaches would be after the fact, and may be of limited value in preventing the threats associated with privacy breaches.

In Canada, there have been attempts to address a number of relevant issues, including prohibiting the non-consensual distribution of intimate images, allowing courts to order the takedown of such images, and awarding compensation (Government of Canada, 2014). In Ireland in 2020, it became a crime to share intimate images without consent under the Harassment, Harmful Communications and Related Offences Act (2020). Known as 'Coco's Law', the Act criminalises such behaviour - online and offline. Importantly it also enables the protection of victims' anonymity and expressly applies to "electronic communications". There are two

new offences created under the act relevant to the use of 'revenge porn' as a tactic to threaten or shame women journalists into silence (Kelleher and Daly, 2021):

- Distributing, publishing or threatening to distribute or publish intimate images without consent with intent to cause harm or being reckless as to whether harm is caused. Crucially, it is irrelevant that a person may have consented to the taking of an image if it is subsequently published or distributed without their consent. This offence will carry a maximum penalty of an unlimited fine and/or seven years' imprisonment.
- Recording, distributing or publishing intimate images without consent. This is a strict liability offence as the person who records, distributes or publishes the image without consent, does not need to have intended to cause harm. The maximum penalty for this offence is EUR €5,000 and/or 12 months' imprisonment.

The inclusion of a strict liability offence in Section Two of the Act is also notable, as the prosecution does not need to prove intention, knowledge, recklessness or even negligence (Hashmall, 2017). Under Section 4 of the same act, it is also now a criminal offence to distribute, publish, or send a threatening or grossly offensive communication (Harassment, Harmful Communications and Related Offences Act, 2020). Convictions under this Section of the Act attract fines and/or a prison sentence of up to two years.

In Brazil, Law No. 12,737/2012, popularly known as the 'Carolina Dieckmann law', was introduced in 2012 after nude photos of the Brazilian actress were hacked and shared after a failed attempt to blackmail her. The law classifies digital crime, including hacking a computer device to obtain, tamper with, or destroy data or information without the authorisation of the device's owner (Glickhouse, 2013). This broadened the scope of the computer intrusion crime under this law, by punishing any form of unauthorised access into a third-party device (Freedom House, 2016a). However, the law's penalties have been described as too "weak to be a deterrent - with just three months to one year in prison and a fine" (Thompson and Muggah, 2015). Law no. 12.965/2014, also known as the Marco Civil Law or 'Constitution for the Internet' (Presidência da República, 2014) offers detailed privacy protections pertaining to personal data, guarantees net neutrality, and promises to uphold the participatory nature of the internet (Freedom House, 2016a). Some online violence victims have filed claims under these laws relating to privacy breaches.

In Mexico, the Olimpia Law on online safety was passed in 2018. Named after Olimpia Melo, a survivor of online violence and advocate for a free and safe internet, it bans crimes against privacy (the dissemination of intimate content without consent) and cyberbullying (including online sexual violence). New crimes were recognised in the state Penal Code, including 'violation of sexual intimacy' (Article 182) and 'crimes against sexual intimacy' (Article 225). However, the laws have been criticised by feminists as failing to respond to women's needs, both theoretically and practically. And there are also concerns about the gap between legislation and implementation (Aguirre et al., 2020). Between 2017-2020, 2,143 investigations were launched into the crime of disseminating intimate images without consent. 83% of the investigations were still in process at the end of

2020. Only 175 of the case files were settled through alternatives to justice, such as conditional suspension of the process, reparatory agreement, or abbreviated procedure (ibid).

7. Prosecuting acts of doxxing

Doxxing as part of online violence against women journalists is also correlated with additional offline risks. Some academics argue that conventional legal instruments do not provide a reliable remedy for victims of doxxing. While doxxing often implies threats by releasing personal information that could invite physical harm, the act of releasing personal data often does not explicitly include threats, meaning that conventional harassment and stalking laws do not apply (MacAllister, 2017). Also, some information revealed by doxxing might already be on the public record, and current legal frameworks in many jurisdictions effectively give immunity to perpetrators (ibid). However, at least one successful prosecution of a perpetrator who doxxed a woman journalist - South African editor Karima Brown discussed in point 8. below - has been identified.

In Sri Lanka, some digital crimes may, in part or whole, fall under general laws, such as the Computer Crimes Act (No. 24 of 2007) which also prohibits hacking, or the Obscene Publications (Amendment) Act (No. 22 of 1983). But these provisions are focussed on e-commerce, and so are not clearly useful to journalists trying to secure prosecution of doxxing for example (Samaratunga and Hattotuwa, 2014). Two agencies currently investigate cybersecurity related crimes. One of them, the Sri Lanka Computer Emergency Readiness Team (CERT), is the first point of contact for individuals reporting threats and vulnerabilities in computer systems and online networks, such as fake accounts, hacking, image-based abuse, and cyberbullying amongst others. CERT provides advice on information security, privacy violations and identity theft, and refers victims of online violence to the police or the Criminal Investigation Department (CID); however, there are no specific provisions for addressing journalists' complaints within these systems, according to a Sri Lankan journalist interviewed for this study who wished to remain anonymous. CERT told her to take her case of identity theft to the CID, who then referred her to their Cyber Crimes division, who told her that they could not take action because they had never encountered such a complaint before, and it had not caused her financial loss. She said she then took the issue to the Telecommunication Regulatory Commission of Sri Lanka, who referred her back to the CID.

8. Electoral and equality law

The South African Electoral Code was the basis for successful legal remedy in a novel legal challenge on behalf of an editor who was doxxed by a political leader and experienced a torrent of online abuse in response. In 2019, the Gauteng High Court in Johannesburg ruled in favour of the late political editor Karima Brown, whose phone number was published on Twitter by a political party's leader, along with claims that she was a State intelligence operative, triggering threats of rape and other acts of violence from self-described party's supporters. The court found that the party's failure to condemn the harassment of Brown breached the Electoral Code's requirement to respect the rights of women and the news

media, and instructed the party and its leaders needed to take reasonable steps to condemn and stop the harassment experienced by the journalist (Columbia Global Freedom of Expression, 2019).

Brown was awarded the equivalent of USD $7,000 in damages and the court ordered the party to formally apologise and delete offending messages from all platforms. Following the verdict, Brown said: "This is a victory for media freedom, a victory against sexism, and it is a victory for women in journalism, and protection, and freedom of the media" (Chabalala, 2019a). This judgement highlights the ways in which electoral law could be used to prosecute cases of online violence and, importantly, potentially work as a deterrent against attacks instigated by political actors.

In another test case from South Africa involving the same political party, the Equality Court ruled against a claim brought on behalf of several journalists, including Daily Maverick investigative journalist Pauli van Wyk who participated in this study. The South African National Editors' Forum (SANEF) took the party to the Equality Court in 2019 to argue that the party had enabled an environment of intimidation and harassment of journalists. SANEF lost the case, with the Equality Court deciding the case did not fall within its terms of reference (Chabalala, 2019b).

9. Copyright Violations

Some legal practitioners have used copyright laws in an attempt to address gendered online violence. In the US, for example, lawyers have used notice and takedown provisions under the Digital Millennium Copyright Act (DMCA) (MacAllister, 2017). However, this is limited to content owned by a victim of harassment, such as selfies or other content they produced themselves. Copyright remedies would not extend to content filmed, consensually or not, by someone else (Chen, 2016). This also makes the role of copyright problematic as a remedy for harassment against women journalists involving so-called 'revenge porn' (i.e. sexual imagery shared without consent to damage a woman's reputation, or to cause shame). There are instances of women journalists being threatened with the release of such content in several countries (Columbia Global Free Expression, 2020; Walsh, 2020).

Facebook was widely criticised for asking users to send their intimate pictures to the platform in its attempt to automate the removal of such images during a 2017 experiment. The company asked users to pre-emptively submit their pictures so that it could detect images posted elsewhere on the site and automatically take them down (Solon, 2019). Some critics raised privacy concerns, others noted that a third person would have to see the images, but some supported the move, saying it gave users agency (ibid).

The copyright remedy is also limited by the nature of the internet. Once images or private information are published online, the author can quickly lose control of the content as it is screen-grabbed, copied and disseminated, limiting the capacity of copyright takedowns to remove it. Further, some legal academics

note that using copyright laws in this way distorts its rationalisation, which is to stimulate the creation of new works by ensuring fair compensation, rather than the suppression of content (ibid).

10. Limitations of conventional communications legal instruments

In the US, for example, laws governing traditional communication methods could arguably address cases of gendered online violence. The Interstate Communications Act provides that anyone who "transmits in interstate or foreign commerce any communication or any threat to kidnap any person or any threat to injure the person" will be fined or imprisoned up to five years, or both (Lipton, 2011). However, this arguably would not extend to other kinds of threats made about a person, nor necessarily apply to social media content. Such limitations are familiar in many jurisdictions internationally.

11. Heavy costs

Other obstacles to legal remedy identified by legal academics researching gendered online violence include the prohibitive costs of bringing a case or justifying prosecution. Quantifiable costs include legal fees, lost income and protection services. Some economic impacts are harder to quantify, including the time, effort and mental well-being imposed by reporting online harassment and abuse to the police. For example, in circumstances where prosecution for acts of online violence requires proof that the conduct was repetitive or ongoing, evidence gathering can be particularly onerous: "One victim described spending 'countless hours' over four years logging the online activity of one particularly committed cyberstalker, 'just in case' he carried out his threats" (Marshak, 2017).

Several journalists interviewed also raised concerns about the capability of law enforcement and judicial investigators to investigate online violence. In Serbia, journalist Jovana Gligorijević was required to submit supporting evidence (such as screenshots, time-logs, etc) on a CD-rom to verify online threats from far-right actors because the Prosecutor for High Tech Crimes was not able to access social media (including YouTube) from their premises, she said. After months of delay and a lost evidence dossier, a police officer asked for Gligorijević's help to review the materials documenting the threats because he did not know how to use social media. In Lebanon, former investigative journalist Myra Abdallah filed a complaint with the Cybercrimes Bureau about death threats she had received, but the case was dropped. "I was told we don't know who [the fake accounts] belong to and the real accounts we cannot do anything about! I was told 'you seem to be messing with the wrong people'," she said. BBC disinformation reporter Marianna Spring had similar experiences in the UK, when she reported rape and death threats to the police in 2020.

This underscores the need for law enforcement to significantly improve the digital investigative capabilities of officers and units assigned to deal with cases of online violence against women journalists. But it also highlights the value of news organisations and civil society actors investing in systems that enable

secure third-party documentation of abuse to relieve the victim of the burden. Related to this, is the burden imposed on victims to 'relive' their online violence experiences for the public judicial record in the course of conventional legal redress. Victims may be reluctant to make complaints or give evidence in court as a result (Lipton, 2011).

The international legal NGOs Media Defence and ARTICLE 19 have also been exploring options for strategic litigation against perpetrators and facilitators of online violence against women journalists as of the time of writing in mid-2021. However Joanna Connolly, former Legal Officer for Media Legal Defence Initiative, noted that they were having difficulty surfacing cases involving women journalists who were prepared to put themselves through onerous litigation processes.

"In the cases that we've taken, the women have faced greater threats and greater reprisals, specifically because they tried to take legal action, specifically because they approached the police...in the environments we work in, that worsens their situation," she said. Meanwhile, irrespective of legal developments, there is mounting public and industry pressure on the social media companies to do much more, and more rapidly, to protect the rights of their users, and in particular those of women journalists, as part of their obligations under the Ruggie Principles.

12. Legislating against online violence

The UK's Online Harms White Paper (DCMS, 2020) which led to the Draft Online Safety Bill (DCMS, 2021) is an example of an attempt to protect people from online violence, which could be relevant to the case of women journalists. The UK government would be obligated to make social media companies uphold their 'duty of care'. This would in turn be overseen by the UK's main independent communications regulator, Ofcom. As the bill stood at the end of 2021, internet communications companies could be fined up to GBP £18 million or 10% of their global turnover for 'harmful' but 'lawful' content that violates binding corporate commitments to deal with abuse. 'Journalism and democratic political debate' are covered under the protections afforded (Tobitt, 2021b). In mid-2021, the UK Culture Secretary said she would follow a recommendation by the Law Commission - an independent body that reviews laws in England and Wales - to include a 'psychological harm' crime in the bill,[16] with reference to online pile-ons (Law Commission, 2021; Milmo, 2021).

The original UK Online Harms White Paper was also followed by the National Safety Action Plan for Journalists (NUJ, 2021), which includes training and support for police representatives, newsroom leaders and student journalists. But Michelle Stanistreet of the UK's National Union of Journalists, noted: "Even with the laws as they are today, there are mechanisms to tackle [online harassment] and for it to be taken seriously and robustly. They're not deployed or utilised now as much as they should be." There are concerns that the draft law could also be abused by bad faith actors to jeopardise freedom of expression, according to UK-based human rights lawyer Caoilfhionn Gallagher KC. ARTICLE 19 has raised similar concerns that the draft lacks an effective notice and appeals process

16 At the time of writing the UK's Online Safety Bill sat with a Joint Committee to assess the legislation (Dawood, 2021).

for content moderation decisions, transparency and accountability. "The draft Bill not only addresses various types of illegal content but also introduces the extremely problematic concept of 'legal but harmful,' which threatens protected expression" (Caster, 2021).

Nigeria's 1999 Constitution guarantees the right to freedom from discrimination on the grounds of sex and recognises women's equal rights. While the country has a National Gender Policy aimed at protecting women from all forms of oppression (Tijani-Adenle, 2019), there is a lack of a legal framework for safeguarding women online. This is seen as contributing to the under-reporting of gender-based harassment (World Wide Web Foundation, 2015). Journalist Kiki Mordi received online death threats for a documentary which exposed her to escalating online harassment (Asamoah, 2019). She chose not to report the attacks, even though she knew she had legal grounds: "The legal process isn't straightforward…I wasn't ready for that. Plus, I didn't have the money to start legal battles or the time to stay off work. I'm freelance, so every second counts".

A Group of Experts on Action against Violence against Women and Domestic Violence, who evaluated legislative measures introduced in Serbia to meet the requirements of the Istanbul Convention, found both the implementation of sexual harassment and stalking laws have often been hampered by significant media backlash. There had been a trivialisation of these offences within public discourse "as the criminalisation of flirting", and a general lack of understanding of the essence of stalking and sexual harassment (GREVIO, 2020).

Germany passed a law in January 2021 reinforcing police powers to investigate online hate speech. Likewise, in France, a new Act called Reinforcing Respect of the Principles of the Republic, which includes provisions on online hate was passed. In September 2021, the European Commission also adopted a Recommendation on the protection, safety and empowerment of journalists which is intended to encourage Member States to take further legal steps to ensure safer working conditions for all media professionals, free from fear and intimidation, whether online or offline.

13. Legislating against misogynistic hate speech

A number of jurisdictions have attempted to legislate against cyberbullying and cyberharassment, which may extend to the harassment of female journalists. However, one of the key legislative gaps identified in this research was the exclusion of sex and gender from anti-hate speech legislation, which routinely covers race, ethnicity, religion, sexual orientation and sometimes transgender identity. Some of the states studied in this research, where gender and sex were excluded from existing hate-speech legislation, include Poland, Sri Lanka, Sweden, and the UK.

In 2021, the US Congress enacted a hate crime bill giving specific protection to Asian-Americans and Pacific Islander people, but this does not recognise misogyny as a hate crime and so does not specifically help women journalists to take action in reference to sex- or gender-based hate speech (Sprunt, 2021; White House, 2021).

From January 2020, the Sri Lankan Defence Ministry began work on new cybersecurity legislation to tackle online defamation as well as ethnically and religiously sensitive posts that incite hatred and pose a threat to national security. This Cyber Security Act was proposed following the Easter 2019 terrorist attacks on churches and hotels which resulted in anti-Muslim violence in the country (Bemma, 2019). It would also address crimes including revenge porn and hacking (Ministry of Defence, 2020). However, there is no specific legislation to protect women journalists from digital violence in Sri Lanka, according to Professor Prathiba Mahanamahewa, Dean of Law and former Human Rights Commissioner of Sri Lanka. While Sri Lanka's Penal Code Article 153 criminalises hate speech which promotes enmity between groups on the basis of religious, racial, language, region, caste or community difference, it does not address gender-based hate (Sri Lanka Government, 1885).

In Brazil, hate speech can be framed as a crime against 'honour', including false accusations and defamation, under Articles 138, 139 and 140 of the Brazilian Penal Code (IRIS, 2019), and it can also be understood as a crime against the public peace (Articles 286 and 287). The Anti-Racism Act (Law No. 7716/1989) criminalises the practice or incitement of discrimination on grounds of race, religion, or national origin (Presidência da República, 1989), and there have been prosecutions for online hate speech under these laws. In 2018, a high profile misogynist was sentenced to 41 years in prison for inciting racism, and making death and terror threats, particularly against women (Uchoa, 2019; Declerq, 2018). His most prominent target was the author of feminist blog 'Write Lola, Write', Lola Aronovich, who has endured years of harassment and threats since 2011. At the time, Aronovich's local Women's Police Station told her it was "unable to carry out investigations", as they involved complex actions such as accessing a website hosted abroad. The Federal Police told the professor of English Literature at the Federal University of Ceará it was "not their job to investigate this type of crime" (Declercq, 2018). But following the man's conviction, 'Lei Lola' [17] ('Lola's Law') (Presidência da República, 2018) was introduced allowing "the federal police to take over any investigation into online crime of a misogynistic nature" and makes hate speech against women illegal (Evans and Coelho, 2019).

France has also adopted a gender-sensitive law addressing 'cyberharassment', which "criminalises the repeated targeting of an individual with both sexual and sexist statements that harm the victim's dignity through their degrading, humiliating, intimidating, hostile or offensive nature" (McCully, 2019). This was in part a response to a Facebook group, created by male journalists in 2009, called the 'League of LOL' (Ligue du LOL) which was found to be harassing women journalists, among others, and encouraging pile-ons (RFI, 2019). Illegal content can also be reported and complaints filed on the platform PHAROS,[18] hosted by the French national police force where officers are trained to track the IP addresses of online attackers that hide behind a pseudonym (INSI et al., 2021).

It appears evident that to be an effective deterrent to online violence, hate speech legislation needs to cover misogyny if women are to protect themselves from

17 13.642/2018

18 'Platform for Harmonisation, Analysis, Cross-referencing and Orientation of Reports': https://www.interieur.gouv.fr/Archives/Archives-publications/Archives-infographies/Securite-des-biens-et-des-personnes/Securite-des-biens-et-des-personnes/Cybersecurite/PHAROS

gender or sex-based hate speech, if they are not able to claim protection under other hate speech categories.

Conclusion:

The UN and other international and regional bodies set clear guidelines and frameworks about the obligations of states to introduce laws to protect women journalists against online harassment. However, in practice, women journalists face a series of barriers and obstacles when seeking to prevent and/or remedy online harassment.

Existing laws are often out-dated and ill-equipped to deal with the modern realities of reporting in the internet era. The need for physical proximity, the need for repetition, defining what constitutes "real" threats, and the inability to identify perpetrators make achieving justice for victims of online harassment difficult to attain.

The additional emotional, financial and time costs faced by women is another barrier. Online harassment of women journalists is a global issue, which makes the prosecution of harassment across jurisdictional and global border lines extremely difficult. Women journalists have often had to resort to creative legal remedies and procedures, which were not designed for online harassment, such as copyright legislation and privacy laws.

Third party platforms, where the harassment often takes place, are often uncooperative or protected by freedom of speech laws or corporate interests. And while more and more countries are beginning to legislate against online violence, misogyny is often omitted or excluded in anti-hate speech laws. Against this background, recommendations at the end of this report, and a 25-point assessment tool, are provided as ways forward for States to improve legal protection of women journalists subjected to online violence.

Recommendations for Action

Individual states could:

1. Ensure that laws and regulations that could protect women journalists offline are applied equally online.

2. As urged by UN General Assembly resolution A/RES/74/157 (2019), collect and analyse "...concrete quantitative and qualitative data on online and offline attacks or violence against journalists, that are disaggregated by, among other factors, sex...". Create a national evidence database tracking perpetrators of online violence against women journalists.

3. Consider introducing protocols and guidelines to restrain elected representatives, their staff, and other officials who engage in gendered online violence against women journalists, with punitive measures attached, and ensure prosecution of those who perpetrate attacks.

4. Consider measures to make social media companies more clearly accountable for combatting online violence against women journalists. Arrive at a clear legal definition of what social networks and messaging services are, and how they are regulated under national laws, with a view to regulating for the protection of women journalists and other human rights defenders working on these platforms (in alignment with the 25-step protocol presented in the parallel publication of comprehensive recommendations associated with this study.).

5. Consider taxing social media companies to provide revenues that could help fund the work of monitoring, protection and training relevant to online attacks on women journalists.

6. Consider measures to make companies more clearly accountable even in countries where these entities are not directly incorporated. This could include a requirement to provide adequate reporting and response mechanisms in the languages on their services, as well as adequate provision of a timely appeals mechanism and recourse to an independent national ombudsperson to help arbitrate cases where platforms and journalists cannot reach a settlement.

7. Consider regulating for the availability and comprehensive functionalities of tools that enable users to easily report online violence to the platforms and escalate appropriately, but ensure such regulatory and legislative interventions respect freedom of expression (refer to the 25-step protocol in the parallel publication of comprehensive recommendations associated with this study.).

8. Require social media companies to notify users who have reported online violence, on what actions have been taken, when and why/why not. These responses could include referrals to informed civil society organizations and effective resources (e.g. the Online Violence Response Hub).

9. Introduce clear and effective transparency regulations for the companies with respect to: gender disaggregation in their reporting content moderation statistics; changes in detection and moderation algorithms; the number and types of notices received and acted upon in a given period; the volume and topics of local content that have attracted labels, distribution restrictions, warnings, demonetisation measures, or content

that has been removed or restricted in circulation, and the numbers and types of users who have been suspended or de-platformed. Additional useful data points could include the number of users and engagement on a national level, as well as revenues in the national market.

10. Regulate to require transparent and gender-disaggregated reporting regarding 'takedown' notices connected to targeted online violence against women journalists, and protection of victims of doxxing and the distribution of sexual imagery shared non-consensually.

11. Establish or reinforce independent national bodies/regulators to oversee compliance with the relevant national and international laws and regulations designed to defend the safety of women journalists.

12. Introduce regulation that provides victims of online violence with access to appeals against company (in)action through an independent, national ombuds facility.

13. Regulate against the social media 'black market', which enables coordinated attacks through sale of accounts, views, likes, and comments.

14. Strengthen labour laws and universal health care to help support women journalists, especially those in precarious employment, when they are targeted in online violence campaigns which involve attempts to get them fired from their jobs.

15. Remedy possible jurisdictional issues by allowing legal action based on the victims' location, rather than the alleged perpetrators', to allow for action against harassment that originates in different locations.

16. Consider introducing legislation such as Ireland's Harassment, Harmful Communications and Related Offences Act 2020, which criminalises the publication and distribution of threats or "grossly offensive" messages with the intention to cause harm. (Any such legislation should reflect the 25 principles for preserving freedom of expression in the context of legislative countermeasures that are laid out separately, emphasising transparency, necessity and proportionality).

17. Regulate, where needed, to preserve the anonymity of complainants and offer closed court proceedings for trials, to encourage more targets of gendered online violence (including acts of 'revenge porn') to come forward without fear of drawing further attention to the abuse;

18. Review the utility of 'shield laws' that protect third-party internet platforms hosting harassing content from civil liability.

19. Ensure hate speech legislation covers both gender and sex (in addition to race, ethnicity, religion, and sexual orientation) to combat misogynistic expressions of online violence, and provide access to additional opportunities for legal redress for women journalists subjected to misogynistic hate speech.

20. Review laws in order to deal with 'pile on' forms of harassment through a 'proportionality' requirement in online harassment indicating whether a one-off comment could cause lesser or greater harm to the victim.

21. Criminalise doxxing and threats to doxx women journalists.

22. Allow legal action on the basis of complaints from third parties (e.g. bystanders or employers) to avoid the onus being on the victim of gendered online harassment to file a complaint.

23. Help fund pro bono legal services specially equipped to deal with gendered online violence so as to alleviate the costs of litigation and increase the likelihood of successful court action brought by women journalists against online violence perpetrators.

Political parties and other political actors could:

24. Desist from mounting attacks (on- and offline) on women journalists, recognising that such conduct can trigger or dangerously inflame threats to their safety.

25. Develop policies, procedures and guidelines requiring party members and officials to avoid instigating, facilitating or fuelling attacks against women journalists.

26. Sanction members and officials who take part in acts of online violence in general and particularly against women journalists.

27. Introduce training modules for party members, including highlighting responsibilities as stakeholders.

Law enforcement agencies and judicial actors could:

28. Acknowledge the connection between online violence and offline harm for targeted journalists, including the risk of escalation to sexual assault and murder, but also serious psychological injury.

29. Understand that online violence is not 'virtual'. It does not have to inflict physical harm to be serious: it causes significant pyschological injury, economic impacts, and reputational damage.

30. Participate in expert-led education programmes for judicial actors and law enforcement agents to improve their media and information literacy as regards

digital freedom of expression and the implications of online violence for press freedom and the safety of women journalists.

31. Participate in expert-led education programmes for law enforcement officials, including police, on the best gender-aware responses to initial reports of targeted online violence against women journalists.

32. Improve social media literacy to support basic knowledge of the operation of contemporary digital media systems, and develop basic digital investigative skills.

33. Recognise the targeted harassment of women journalists online as a workplace safety issue.

REFERENCES: A list of references consulted for this study has been published by ICFJ[19]

19 https://www.icfj.org/sites/default/files/2022-05/UNESCO%20Annexe%201_%20Bibliography.pdf

A NOTE ABOUT OUR METHODOLOGIES

The survey method adopted was 'purposive sampling', with 'snowballing' techniques used to generate responses within the international field of journalism. The results, therefore, are not generalisable, although it is legitimate to extrapolate many patterns that may well have wider applicability. To avoid illegitimate or inauthentic responses and ensure data integrity, the survey was distributed digitally via the closed networks of UNESCO and ICFJ, our research partners, civil society organisations focused on media development, journalism safety and gender equality, and groups of professional journalists. The survey ran from September 24th to November 13th 2020 and it garnered 901 valid responses. The survey results were then disaggregated along gender lines, and a subset of data from 714 respondents who identified as women was isolated for analysis. In parallel, we identified 183 interviewees through the survey and institutional outreach, as well as via the networks of the research team. The interviews were conducted face-to-face (where COVID-19 restrictions allowed) and via digital channels. Most of the interviews were undertaken synchronously by the researchers identified in this report. The vast bulk of interviewees chose to be publicly identified after being offered the option to remain anonymous.

For the big data case studies on Maria Ressa and Carole Cadwalladr 2.5 million social media posts were collected over the course of five years and 13 months respectively. Relevant subsets of these collections were identified for network analysis and deeper investigation via Natural Language Processing (NLP). The results were synthesised with the long form qualitative interviews and contextualised via detailed timelines developed through desk research.

The University of Sheffield (UK) granted ethics clearance for the English language version of the survey and English language interviews. Translations of the survey into other languages were conducted by UNESCO and reviewed by ICFJ. The University of Sheffield also provided ethics clearance for quantitative data gathering and analysis associated with the big data case studies featured here.

unesco

in cooperation with

ICFJ International Center for Journalists