WORLD BANK GROUP
Development Economics | Global Indicators

Global Indicators Briefs No. 18

Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws

Nelsy Reyhanne Marikel Affoum, Isabel Micaela Santagostino Recavarren, Nayantara Vohra, and Quentin Wodon

Cyber violence against women has been rising at alarming rates in recent decades. Such acts not only harm women as individuals but have severe detrimental effects on society and the economy at large. This Brief analyzes laws from 190 economies to assess the extent and coverage of current legislative safeguards for women from cyber harassment, one of the many forms of cyber violence. Data collected by the World Bank Group's *Women, Business and the Law* project reveals that laws that protect women against cyber harassment exist in only about one-third of economies, covering less than half of the population of children, adolescent girls, and women. Enhancing legal protections is crucial to effectively tackle cyber violence against women.

Laws addressing cyber harassment are necessary

As internet, social media, and mobile connectivity have rapidly expanded their reach, online violence has also emerged and has become alarmingly widespread. Violence against women has seeped into the online space, targeting women and girls in multiple forms, including cyber harassment or bullying. A phenomenon that was unimaginable thirty years ago is now showing its harmful health, social, and economic consequences.

Gendered cyberviolence further widens the pre-existing, gender-related digital divide by creating barriers to equity and full participation online (Jane 2020). Studies have found that women are more likely than men to experience severe forms of online violence, such as cyber harassment and stalking (Brody and Vangelisti 2017). Such abuse often has far-reaching consequences. For instance, online violence has been found to be a pervasive problem faced by women not only in the private sphere, but also while engaging in politics, journalism, and activism, thereby posing a significant barrier to their political participation and freedom of expression. Further, women who come from traditionally marginalized sections of society are the most vulnerable and are often the target of some of the most violent and vicious online hate campaigns (Di Meco 2023). As legislation addressing online violence is still lacking or absent in most economies, many women and girls are left unprotected without redress measures. While recognizing that all forms of cyber violence are widespread and have a negative impact on women and girls, this Brief focuses specifically on cyber harassment and bullying given their pervasiveness and considerable increase recently and, in particular, during the pandemic (Shoib et al. 2022).

Women, Business and the Law (WBL) analyzes how laws and regulations affect women's economic opportunities in 190 economies. The analysis presented in this Brief is a result of research undertaken by the WBL team in 2021 and 2022 to understand how current legislation safeguards individuals online. The research resulted in a new dataset of 7 questions (box 1), across 190 economies, measuring the presence or absence of legislation on cyber harassment, cyber-sexual harassment, and redress mechanisms and related procedures, as well as whether vulnerable segments of the population—such as children and people with disabilities—are considered within the context of those laws. The goal is to shed light on the need for the adoption of comprehensive legislation to prevent online violence and ensure a safer online environment for all.

What is cyber harassment and bullying?

It is estimated that one in three women worldwide experiences physical or sexual violence in their lifetime (WHO 2021). Likewise, cyber violence against women and girls, and in particular cyber harassment and bullying (see definition in table 1), have risen to disturbing levels. Studies suggest that in the European Union, for example, 73 percent of women have been targeted by online abuse (EU Agency for Fundamental Rights 2014). A German survey of more than 9,000 national internet users, ages 10 to 50, also found that women are significantly more likely than men to experience cyber harassment and stalking (Staude-Müller, Hansen, and Voss 2012). The United Nations (UN) estimates that 95 percent of aggressive behavior, harassment, abusive language, and denigrating images in online spaces are aimed at women. The COVID-19 pandemic has only intensified violence against women and girls (VAWG). While the sharp increase in intimate partner violence during the pandemic made their physical environment less safe (UN Women 2020b), simultaneously the online world also became more dangerous for women and girls due to the increased reliance on technology and virtual communication during the pandemic (UN Women 2020c). Since the outbreak of COVID-19, reports of online abuse and bullying in Australia, for instance, have increased by 50 percent (UN Women 2020a). A study by Plan International covering 22 economies additionally reported that a staggering 58 percent of girls and women personally experienced some form of online violence in 2020 (Plan International 2020).

Due to the fast-paced advancement of information and communications technology (ICT), terminology around online

Affiliations: *Nelsy Reyhanne Marikel Affoum, Isabel Micaela Santagostino Recavarren, and Nayantara Vohra are with World Bank, Development Economics. Quentin Wodon is with UNESCO IIBA. For correspondence: isantagostino@worldbank.org, nvohra3@worldbank.org,or naffoum@worldbank.org.*
Acknowledgements: *This Brief would not be possible without the contribution of the World Bank Group's Women, Business and the Law team. The authors would like to thank Tea Trumbic and Norman Loayza for comments and guiding the publication process. David C. Francis and Nancy Morrison provided excellent editorial assistance.*

Box 1 Research questions on cyber harassment and bullying

The analysis in this Brief is based on the following seven questions:

1. Are there any legal provisions on cyber harassment and bullying?
2. If Yes, does the law on cyber harassment/bullying explicitly mention sexual harassment?
3. Are there any penalties for cyber harassment/bullying?
4. Are there any civil remedies/redress measures for the survivor?
5. Are there any special procedures for cases of cyber harassment/bullying?
6. Does the law address cyber harassment/bullying against women with disabilities?
7. Does the law address cyber harassment/bullying against children?

Importantly, this assessment of legal protection against online violence for women and children is based solely on the letter of the law and not on its application or enforcement, which is outside the scope of this analysis. *Women, Business and the Law* recognizes that while having laws on the books is important, it is not sufficient. In many places, adequate laws may coexist with a high prevalence of online violence. This may result from poor implementation of laws, whether due to poor enforcement; low capacity; or the lack of additional mechanisms, policies, or specific programs or interventions that address the underlying issues. Thus, legal protection does not necessarily reflect effective protection from violence but is an important first step.

Table 1 Terminology: Forms of cyber violence or online violence

Behavior	Definition/examples
Cyber (sexual) harassment and bullying	Unwanted verbal or nonverbal conduct of a sexual nature online with the purpose or effect of violating the dignity of a person by creating an intimidating, hostile, degrading, humiliating, or offensive environment (Šimonović 2018). Specific acts that constitute cyber (sexual) harassment and bullying include: • Offending a person online by sending unwanted, offensive, sexually explicit emails, messages, or advances online, threats of violence, or hate speech (EU Agency for Fundamental Rights 2014). • A persistent and repeated course of conduct targeted at a specific person, designed to cause severe emotional distress and often a fear of physical harm.
Cyber stalking	The repeated pursuit of an individual using electronic or internet-capable devices (Reyns, Henson, and Fisher 2012). Such repeated pursuits may be threatening, coercive, or intimidating (Hazelwood and Koon-Magnin 2013). Specific acts that constitute cyber stalking include: • Repeated unwanted communications; repeated unwanted sexual advances or requests; repeated threats of violence; and surveillance and monitoring of a victim's location, daily activities, and/or communications through computer software and mobile phone applications or global positioning system (GPS) location information (Henry and Powell 2016). • One user repeatedly sending unwanted e-mails or text messages to their victims. • Sexual advances or requests, threats of violence, and surveillance of a victim's location through a variety of technologies.
Online gender-based hate speech	Any supposition, belief, assertion, gesture, or act that is aimed at expressing contempt toward a person, based on their sex or gender, or to consider that person as inferior or essentially reduced to their sexual dimension. It includes expressions that spread, incite, promote, or justify hatred based on sex (Council of Europe Gender Equality Strategy 2016). Hate speech campaigns are often efficiently organized, in which multiple perpetrators simultaneously target the same victim or group of victims by. Specific acts that constitute online gender-based hate speech include: • Victim blaming and revictimization; "slut-shaming"; body-shaming; "revenge porn" (the sharing of explicit or sexual images without consent); brutal and sexualized threats of death, rape, and violence; offensive comments on appearance, sexuality, sexual orientation, or gender roles; false compliments or supposed jokes; using humor to humiliate and ridicule the target (Council of Europe Gender Equality Strategy 2016). • All forms of expression that share, encourage, promote, or justify race hatred, xenophobia, anti-Semitism, or every other form of hatred based on intolerance, including aggressive nationalism; ethnocentrism; discrimination; and hostility toward minorities, emigrants, or persons of foreign origin (Council of Europe 1997).
Flaming	The deliberate use of heated, emotionally charged, or contrarian statements to elicit a response from another online user. Specific acts that constitute flaming include: • Vitriolic content, denoted by explicit language and misogyny.
Image-based sexual abuse/ nonconsensual pornography revenge porn	The sexually explicit portrayal of one or more persons that is distributed without the subject's consent. These are often committed by a victim's former partner and posted on a specialized website or social media profile. Contrary to its name, this need not be motivated by personal revenge. Perpetrators may be seeking sexual gratification, or want the victim to do something for them, using the images as a form of social or economic blackmail. When the victim is a minor, it is considered child pornography. Specific acts that constitute image-based sexual abuse/nonconsensual pornography include: • Posting or distributing sexually graphic images or videos without consent.
Doxing	The publishing of a victim's personal details and sensitive data online, such as home address, photographs, name, and names of family members (MacAllister 2017). Often employed by cyberbullies and online gamers. Specific acts that constitute doxing include: • Searching, collecting, and publicly sharing personally identifiable information against a target's will.

Source: Council of Europe 1997; Council of Europe Gender Equality Strategy 2016; EU Agency for Fundamental Rights 2014; Hazelwood and Koon-Magnin 2013; Henry and Powell 2016; MacAllister 2017; Meensakshi, Liombo, and Navarra 2021; Reyns, Henson, and Fisher 2012; Šimonović 2018.

violence against women is still emerging. Traditional definitions of violence may not be adequate to address all the forms that online violence may take (Šimonović 2018). The rapid development of digital technology and spaces, including through artificial intelligence, will inevitably give rise to different and new manifestations of online violence against women (Šimonović 2018). Older laws may not account for such acts of harassment committed using mobile phones, the internet, social media platforms, and/or email, among others, and therefore can fail to protect women against this new type of abuse. Further, terms such as cyber harassment, online violence, digital violence, and cyber violence are often used interchangeably and can be confusing. Cyber or online violence, however, is an umbrella term indicating a behavior that may take many different forms, which include, among others, cyber harassment and bullying, cyber stalking, online gender-based hate speech, flaming, image-based sexual abuse, nonconsensual pornography, revenge porn, and doxing (table 1). Such digitally abusive behaviors may be perpetrated by intimate partners, sexual or dating partners, acquaintances, or strangers (Henry and Powell 2016). In a general sense, the definition of online violence against women extends to any act of gender-based violence that is committed, assisted, or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the internet, social media platforms, or email, against a woman because she is a woman, or in a way that affects women disproportionately (Šimonović 2018).

Online or cyber harassment, one of the many forms of cyber violence, has been described as an act or behavior that torments, annoys, terrorizes, offends, or threatens an individual via email, instant messages, or other digital means with the intention of harming that person (Hazelwood and Koon-Magnin 2013). Cyber sexual harassment refers to any form of unwanted online verbal or nonverbal conduct of a sexual nature with the purpose or effect of violating the dignity of a person by creating an intimidating, hostile, degrading, humiliating, or offensive environment (Šimonović 2018). Specific behaviors that may constitute online sexual harassment include sending unwanted, offensive, or sexually explicit emails or messages and inappropriate, offensive advances on social networking websites or in internet chat rooms (EU Agency for Fundamental Rights 2014).

The harms of cyber harassment and bullying may also be economic, social, and physical. A 2021 study conducted in the European Union estimated the cost of cyber violence to be on the order of €49.0 to €89.3 billion (Meensakshi, Liombo, and Navarra 2021). In addition to labor market impacts and health care and legal costs, the monetized value of the loss in terms of quality-of-life accounts for more than half of these estimated costs. Social consequences include a negative effect on women's reputations and livelihoods, and an adverse impact on women's digital inclusion, which pushes them off the internet and prevents them from being active digital citizens. Online violence particularly targets women holding public positions, such as politicians, artists, journalists, or activists, and thus may deter others from seeking such exposure (West 2014). Finally, cyber violence often represents a continuation or prelude to offline violence. Research shows that 70 percent of cyber harassment and stalking victims have also experienced intimate partner violence (EU Agency for Fundamental Rights 2014).

An increasing number of international conventions address cyber harassment

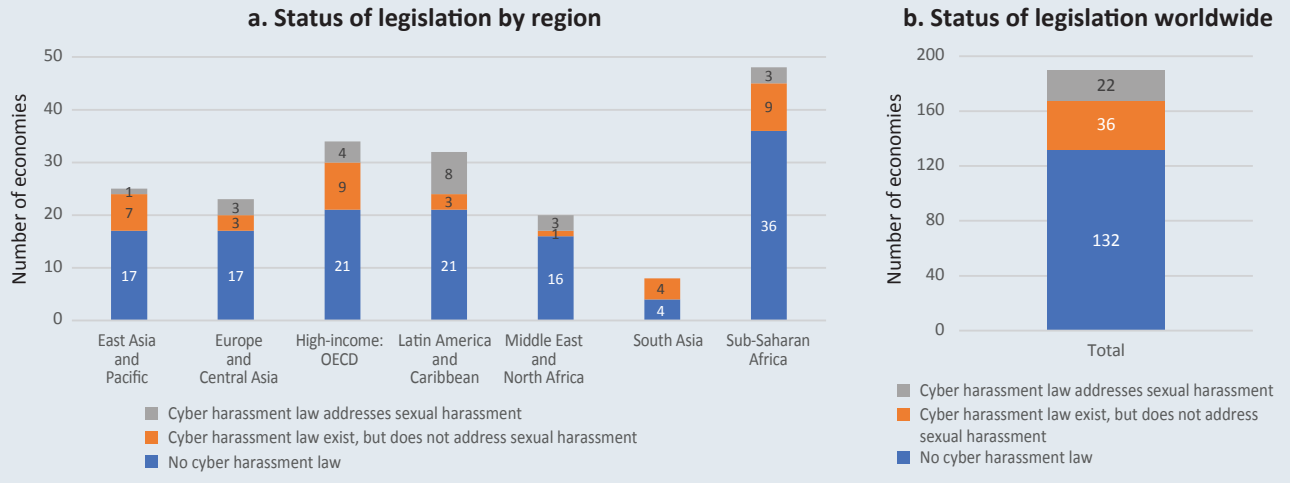
Although there is no international, standard legal framework that specifically governs online violence, various instruments have recognized the intensity of the issue and addressed the necessity to develop clear legislation as well as guidelines for prosecution. Recommendation 35 of the Committee on the Elimination of All Forms of Discrimination against Women (CEDAW) extends the definition of violence against women beyond the physical space to include "technology-mediated environments," thereby addressing online and ICT-facilitated violence against women (CEDAW 2017).

Similarly, the Istanbul Convention on Preventing and Combatting Violence against Women and Domestic Violence by the Council of Europe, provides a comprehensive definition of the types of violence against women, including online and ICT-facilitated violence (Council of Europe 2011; Council of Europe 2021). Moreover, the Council of Europe Expert Group on Action against Violence against Women and Domestic Violence (GREVIO), a body entrusted to monitor the implementation of the Istanbul Convention, notes in its General Recommendation No. 1 on the digital dimension of violence against women that as women increasingly become susceptible to online violence, it should be dealt with in domestic laws and regulations (GREVIO 2021). However, while both the Lanzarote Convention and the Budapest Convention on Cybercrime address sexual exploitation of children occurring online and prosecute cybercrimes in general, they do not address ICT-induced violence against women (Council of Europe 2001).

Only 30 percent of economies worldwide provide legal protections against cyber harassment

Most economies still lack legislation to protect women and girls from cyber harassment or bullying. Given that women are often disproportionately affected by online abuse, strengthening laws that protect against cyber harassment and bullying can significantly help make the online space safer for them. Only 58 of the 190 economies analyzed have enacted some legislation on this topic, meaning that worldwide only 47 percent of women are protected by provisions on cyber harassment (box 2). Overall, such laws are more common in

Figure 1 Only 58 economies worldwide have enacted legislation on cyber harassment, while 22 economies worldwide have enacted legislation on cyber-sexual harassment



Source: *Women, Business and the Law* database, 2022.
Note: OECD = Organization for Economic Co-operation and Development.

high-income economies than in low- and middle-income economies. Yet even in high-income economies, only about one third have such laws. In terms of regions, half of the economies in South Asia have legislation on cyber harassment, followed by OECD high-income economies, with 38 percent. The Middle East and North Africa and Sub-Saharan Africa show the most room for improvement, with 20 percent and 25 percent of economies having such laws, respectively (figure 1, panel a).

Because economies do not necessarily include online sexual harassment in their definition of cyber harassment, only 22 economies globally have established legal protections specifically addressing cyber sexual harassment (figure 1, panel b). There are substantial differences between regions and income groups (box 2). For instance, none of the economies in South Asia and only one economy in the East Asia and Pacific region have enacted such a law. In Latin America and the Caribbean, eight economies out of thirty-two (Belize, Dominican Republic, El Salvador, Guyana, Mexico, Nicaragua, Peru, St. Vincent and the Grenadines) have laws that address cyber sexual harassment.

Good practice legislation should not only define and address cyber harassment and bullying but also clearly describe the types of behaviors prohibited and their impact on the survivor. For instance, Saint Vincent and the Grenadines' Cybercrime Act of 2016 and Uganda's Computer Misuse Act of 2011 describe cyber harassment as the unwanted transmission of information, statements, or images that disturb the peace of the complainant, as well as communication that is obscene, constitutes a threat, or is menacing. South Africa's Protection from Harassment Act of 2011, in addition to defining online harassment, also refers to its impact on the survivor, describing it as a behavior that "causes harm or inspires the reasonable belief that harm may be caused to the complainant." This aspect is fundamental because it provides a survivor-centered perspective and focuses not only on the type of behavior prohibited, but also on its impact on the complainant. Similarly, Nigeria's 2015 Cybercrimes Act, which was passed with the goal of providing an effective and unified legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes, also provides a comprehensive definition of cyber harassment. The law also criminalizes (1) sending messages that are grossly offensive, pornographic, or of an indecent, obscene, or menacing character or (2) sending false messages for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will, or needless anxiety. Therefore, while it is important that laws use specific terms such as "cyber harassment" and "cyber bullying," it is fundamental that laws adequately spell out the type of behaviors prohibited and the impact of such behavior on survivors.

Only 27 percent of economies have redress measures for cyber harassment

Globally, 53 out of 190 economies impose criminal penalties for offenses associated with cyber harassment. Such penalties often include

Box 2 **Populations of children, adolescent girls, and women protected from cyber harassment and cyber violence under the law**

Table B2.1 presents population-weighted results for children ages 0–14 and women (and adolescent girls) ages 15–64.

Of the 1,968 million children in the economies included in the sample shown in the table, only 211 million (11 percent) are protected by specific provisions related to children in existing laws. Only 47 percent of women are protected by provisions on cyber harassment, and only 12 percent by legislation on cyber-sexual harassment. Very few children or women are protected through civil remedies or redress measures for survivors of online violence. Penalties for offenders are more common, but those do not result in compensatory benefits for survivors. Only 3 percent of women have access to civil remedies for cyber harassment, and 11 percent to special procedures for these types of cases.

Table B2.1. **Number and percentage of children, adolescent girls, and women protected from cyber harassment under the law as of 2021**

	Global	Regions[a]							Income Groups			
		EAP	ECA	High-income OECD	LAC	MENA	SA	SSA	Low	Lower-middle	Upper-middle	High
	Children ages 0–14 protected											
Children ages 0–14 protected (millions)	1,968	429	88	178	150	136	512	476	271	988	511	199
Any laws on cyber harassment	50%	9%	28%	69%	62%	15%	87%	52%	29%	65%	26%	68%
Specific provisions in the law on:												
Sexual harassment (%)	14%	8%	27%	12%	32%	15%	0%	27%	0%	16%	17%	15%
Penalties for cyber harassment (%)	48%	9%	28%	62%	33%	15%	87%	52%	29%	65%	17%	62%
Civil remedies/redress measures for survivor (%)	4%	0%	0%	2%	23%	0%	0%	9%	8%	2%	7%	2%
Children (%)	11%	0%	24%	11%	3%	7%	15%	17%	18%	9%	8%	14%
Special procedures for cyber harassment (%)	15%	8%	0%	1%	23%	0%	17%	30%	4%	24%	10%	1%
	Women ages 15–64 protected											
Women ages 15–64 protected (millions)	2,473	718	141	353	212	141	594	313	174	1056	861	382
Any laws on cyber harassment	47%	6%	28%	67%	66%	18%	88%	54%	30%	63%	23%	66%
Specific provisions in the law on:												
Sexual harassment (%)	12%	5%	25%	12%	30%	17%	0%	29%	0%	12%	13%	14%
Penalties for cyber harassment (%)	43%	6%	27%	60%	30%	17%	88%	54%	30%	63%	14%	59%
Civil remedies/redress measures for survivor (%)	3%	0%	0%	1%	21%	0%	0%	9%	7%	2%	5%	1%
Women with disabilities (%)	2%	0%	1%	11%	3%	7%	0%	1%	0%	1%	1%	13%
Special procedures for cyber harassment (%)	11%	5%	0%	1%	21%	0%	13%	33%	5%	18%	8%	1%

Source: Compilations using the *Women, Business and the Law* (WBL) data and World Development Indicators database.
Note: This analysis is based on 2021 data for 183 of the 190 economies. Population data by age group are not available for seven sparsely populated economies in the World Bank's World Development Indicators (Dominica, Eritrea, Kosovo, Marshall Islands, Palau, San Marino, St. Kitts and Nevis). The statistics are provided in terms of the population protected under the law. The total population of children ages 0–14 and women ages 15–64 is also provided in the table for comparison purposes. The differences between the reference populations and the individuals protected are those not protected.
a. OECD = high-income member-countries of the OECD (Organisation for Economic Co-operation and Development). In other regional groupings, high-income OECD countries are not included. EAP = East Asia and Pacific; ECA = Europe and Central Asia; LAC = Latin America and Caribbean; MENA = Middle East and North Africa; SA = South Asia; SSA = Sub-Saharan Africa.

imprisonment, a monetary fine, or a combination of the two sanctions. Some economies also prescribe harsher penalties for repeat offenders. In India, for example, the maximum prison sentence for cyber stalking increases from three to five years if the offender has been previously convicted for the same offence. Similarly, in Saudi Arabia, the law prescribes an enhanced maximum prison sentence of five years (as opposed to two years) for recurring offenders. Bulgarian law provides for a longer prison sentence if the acts of cyber harassment were committed in the context of domestic violence. Nigeria's Cybercrimes Act punishes acts of cyber harassment with three to ten years of imprisonment. Israel's Prevention of Sexual Harassment Law, adopted in 1998 to primarily prohibit sexual harassment in the workplace and in education, punishes offenders of cyber harassment with a prison term of up to two years.

Regarding civil remedies, however, very few economies have included provisions in their cyber harassment legislation. Only seven economies (Bhutan, Guyana, Israel, Kenya, Mexico, Trinidad and Tobago, Uganda) provide for either damages or financial compensation (or a combination of both) for victims in addition to criminal penalties. In Kenya, the Computer Misuse and Cybercrimes Act entrusts the court with the power to warrant compensation orders in favor of the victim for any offence under the act. Likewise, in Trinidad and Tobago, the victim is entitled to an order for compensation for loss of earnings, medical expenses, moving or accommodation expenses, and/or legal costs. Israel's law also establishes a civil procedure defined by the country's Torts Ordinance where the court may order compensation for online sexual harassment without proof of damage.

Nineteen economies have established special procedures for cyber harassment

Establishing coherent procedures to ensure the protection of women and children allows victims to follow clearly defined guidelines that will facilitate their quest for justice. Yet among the 58 economies that do have legislation against cyber harassment, only 19 have a defined procedure to deal with cyber harassment cases. These are addressed in cybercrime acts or legislation specifically pertaining to ICT, which tend to provide a procedure that is globally applicable to all ICT-related crimes. In Indonesia, for example, the Law on Electronic Information and Transactions entrusts state police investigators and certain civil servants with the special authority to investigate criminal acts in the field of information technology and electronic transactions. Similarly, in the Philippines, the Philippines National Police Anti-Cybercrime Group (PNPACG) is charged with the implementation of laws on cybercrime. The PNPACG is responsible for receiving complaints of gender-based online sexual harassment, developing an online mechanism for reporting real-time gender-based online sexual harassment acts, and apprehending perpetrators. The national Cybercrime Investigation and Coordinating Center (CICC) also coordinates with the PNPACG to prepare appropriate and effective measures to monitor and penalize gender-based online sexual harassment.

Eswatini's Sexual Offences and Domestic Violence Act protects against cyber sexual harassment but exclusively provides for protection orders to respond to the harm inflicted. Interestingly, the only economy where the violence against women legislation enables victims of ICT-related crimes to obtain protection orders is Mexico. Specifically, the Ley General de Acceso de las Mujeres a una Vida Libre de Violencia establishes protection order procedures that involve the companies operating digital platforms, media, social networks, or electronic pages within this process. Consequently, public prosecutors and judges are empowered to mandate digital platforms, communication media, social networks, or electronic pages to disable user content related to cyber harassment investigations in compliance with the court's order.

It is worth highlighting legislation in Saint Vincent and the Grenadines and South Africa, as both also establish obligations for internet providers. Saint Vincent and the Grenadines' 2016 Cybercrime Act not only provides a detailed definition of cyberbullying, harassment, and sexual harassment, but also establishes how investigations should be carried out and institutes a special procedure. This includes the possibility for the complainant to request and obtain a protection order, which is required to carry out a criminal investigation and the related proceedings. The judge may then order the internet service provider to remove or disable the electronic data, as well as authorize and request warrants. Finally, the law regulates aspects related to the liability of internet service providers. And South Africa's 2011 Protection from Harassment Act, in addition to establishing a procedure for the complainant to obtain a protection order, determines what the court can request from an electronic communications service provider, as well as the provider's duty in such cases. Further, the law establishes a special procedure for online harassment complaints by including terms and type of information the service provider should make available.

Recognizing the complexities involved in prosecuting cases of cyber harassment, several economies have appointed national bodies or agencies with the task of receiving complaints and following up on the implementation of the law. Nigeria's 2015 Cybercrimes Act designated a National Security Adviser as the coordinating body for all security and enforcement agencies under the Act and established a Cybercrime Advisory Council and a National Cybersecurity Fund. Benin established a Regulatory Authority entrusted to oversee the correct implementation of Loi No. 2017-20 and to receive complaints from users and associations of electronic communications services. Moreover, the Act specifically mandates the Regulatory Authority to put in place the material and human resources necessary to process complaints. Similarly, in 2016 the Israeli Cabinet approved a Public Security Ministry initiative designed to include the creation of a special unit under the Israeli police to handle cybercrimes, as well as a national hotline operating 24/7 to handle complaints.

In some cases, procedures enumerated in ICT legislation establish a governing body designated to rule and oversee all aspects related to this area of the law. Usually, a governing body is created to specifically regulate national ICT utilization and a budget is allocated to fund its actions; an authority is entrusted to deliberate on ICT-related crimes; and in some cases, provisions are made for preventive services, such as psychological support for victims or education classes on cybercrimes to prevent the occurrence of offences. For instance, the Malawi Communications Regulatory Authority, established by the Communications Act, regulates the implementation of the Electronic Transactions and Cyber Security Act, and appoints a "cyber inspector" to assess the relevance of the complaint, and, if necessary, proceed with the investigation. It also implements public educational programs on the safe use of the internet to inform the public on cybercrimes, safe internet usage, and remedies and procedures when affected by cybercrimes.

Does the law protect vulnerable segments of the population?

Highly vulnerable segments of the population, including women with disabilities and children, should benefit from additional protections under the law. Intersectional characteristics such as age, race, and disability, among others, make these segments of the population more vulnerable to harassment and mark them out to be targeted more relentlessly. A study found that 14 percent of girls who self-identify as having a disability and who had experienced harassment stated that their abuse occurred because of their condition (Plan International 2020). Yet the data show that among the 58 economies that have legislation on cyber harassment, only 9 specifically protect women with disabilities from cyber harassment. While most provisions are designed to enhance established penalties for offenses committed against a "vulnerable" portion of the population, some laws are designed to address and punish cybercrimes against women with disabilities specifically. El Salvador punishes the dissemination of sexual content through ICT about women with disabilities for a period of four to eight years. In Saudi Arabia, the criminal penalty is increased to a prison term of a period not exceeding five years and/or a fine not exceeding SRls300,000 in cases where the cyber harassment victim has "special needs."

With limited knowledge of the risks and challenges associated with an online presence, children and young adolescents have also increasingly become exposed to cyber bullying and/or cyber stalking (Zhu et al. 2021). To effectively showcase this reality, an analysis executed by the Pew Research Center reports that younger adults between 18 and 29 years old tend to face more severe forms of online abuse than those aged 30 and older, defined by the Center as behaviors

such as being physically threatened, stalked, sexually harassed, or harassed for a sustained period of time (Vogels 2021). Despite these alarming figures, only 21 economies have legislation specifically protecting children from cyber harassment. Much like laws enacted to protect women with disabilities, this legislation enhances pre-existing penalties involving minors. In France, the penalty for sexual harassment is increased by three years of imprisonment combined with a fine of €45,000 when the offence is committed against a person particularly vulnerable due to their age. Two economies, Belize and El Salvador, address children as direct victims in their legislation. Belize's Cybercrime Act of 2020 punishes offenders who utilize a computer system to attempt to directly (1) communicate with a child to engage in a sexual activity or sexual conversation and (2) plan a meeting to engage in a sexual activity or abuse a child. Minors and persons with disabilities are especially protected under Israel's law, where both are listed as categories that may require "special protection" based on their vulnerability. Along the same line, Benin's Loi N°2017-20 establishes harsher penalties if cyber harassment is committed against persons who are vulnerable due to age, pregnancy, disease, infirmity, or physical or mental disability.

Conclusion

Ending violence against women is one of the aims of the Sustainable Development Goals. Achieving this target would end the harm and suffering caused by such violence and have a wide range of beneficial effects, including for economic growth and standards of living. Limited attention has been placed so far on enacting laws to prevent online violence; however, having adequate laws in place is fundamental for more effective responses to cyber harassment. Legal protection under the law is crucial to reduce impunity for offenders and open avenues for redress.

Important findings emerge from the analysis presented in this Brief. Legal protection remains weak in most parts of the world, whether with respect to geographic regions or income groups. Laws exist in only about one-third of economies, and they cover less than half of the population of children, adolescent girls, and women. The assessment is even bleaker when considering specific provisions. While enacting laws is not sufficient to curb online violence, it does send a clear message that cyber harassment and bullying are simply not acceptable.

References

Brody, N., and A. L. Vangelisti. 2017. "Cyberbullying: Topics, Strategies, and Sex Differences." *Computers in Human Behavior* 75: 739–48. https://doi.org/10.1016/j.chb.2017.06.020.

CEDAW (Committee on Elimination of Discrimination Against Women). 2017. "General recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (1992)." United Nations, New York.

Council of Europe. 1997. Recommendation No. R (97) 20 of the Committee of Ministers to Member States on "Hate Speech." https://rm.coe.int/1680505d5b.

Council of Europe. 2001. "Convention on Cybercrime." https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

Council of Europe. 2011. "Council of Europe Convention on preventing and combating violence against women and domestic violence." Istanbul, 11.V.2011. Council of Europe Treaty Series-No. 210. https://rm.coe.int/168008482e.

Council of Europe. 2016. Gender Equality Strategy. "Combating Sexist Hate Speech." https://rm.coe.int/1680651592.

Council of Europe. 2021. Council of Europe Convention on preventing and combating violence against women and domestic violence. "The Four Pillars of the Istanbul Convention." https://rm.coe.int/coe-istanbulconvention-brochure-en-r03-v01/1680a06d4f.

Di Meco, Lunica. 2023. *Monetizing Mysogony–Gendered Disinformation and the Undermining of Women's Rights and Democracy Globally*. She Persisted. https://she-persisted.org/wp-content/uploads/2023/02/ShePersisted_MonetizingMisogyny.pdf.

EU (European Union) Agency for Fundamental Rights. 2014. *Violence against Women: An EU-wide Survey– Main Results*. Luxembourg: Publications Office of the European Union. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf.

GREVIO (Group of Experts on Action against Violence against Women and Domestic Violence). 2021. "GREVIO General Recommendation No. 1 on the digital dimension of violence against women." Council of Europe. https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147.

Hazelwood, S. D., and S. Koon-Magnin. 2013. "Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis." *International Journal of Cyber Criminology*. https://www.cybercrimejournal.com/hazelwoodkoonmagninijcc2013vol7issue2.pdf.

Henry, N., and A. Powell. 2016. "Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law." Social & Legal Studies 25 (4): 397–418. doi:10.1177/0964663915624273.

Jane, Emma A. 2020. " Online Abuse and Harassment." *The International Encyclopedia of Gender, Media, and Communication*. https://doi.org/10.1002/9781119429128.iegmc080.

MacAllister, Julia M. 2017. "The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information." 85 *Fordham Law Review* 2451 (2017).

Meensakshi, F., L. Liombo, and C. Navarra. 2021. "Combating Gender-based Violence: Cyber Violence." European Union, Brussels. European Parliamentary Research Service, European Union, Brussels.

Plan International. 2020. *Free to Be Online? Girls and Young Women's Experiences of Online Harassment*. Plan International. https://plan-international.org/uploads/2022/02/sotwgr2020-commsreport-en-2.pdf.

Reyns, B. W., B. Henson, and B. S. Fisher. 2012. "Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending among College Students." *Deviant Behavior* 33 (1): 1–25.

Shoib, S., S. Philip, S. Bista, F. Saeed, S. Javed, D. Ori, A. Bashir, and M. Chandradasa. 2022. "Cyber Victimization during the COVID-19 Pandemic: A Syndemic Looming Large." *Health Science Reports*, February 17, 2022.5 (2): e528. doi: 10.1002/hsr2.528. PMID: 35224224; PMCID: PMC8851571.

Šimonović, D. 2018. A/HRC/38/47: *Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on Online Violence against Women and Girls from a Human Rights Perspective*. Office of the United Nations High Commissioner for Human Rights (OHCHR). https://digitallibrary.un.org/record/1641160.

Staude-Müller, F., B. Hansen., and M. Voss. 2012. "How Stressful Is Online Victimization? Effects of Victim's Personality and Properties of the Incident." *European Journal of Developmental Psychology* 9 (2): 26074. https://www.tandfonline.com/doi/abs/10.1080/17405629.2011.643170.

UN Women. 2020a. *From Insights to Action: Gender Equality in the Wake of COVID-19*. UN Women. https://www.unwomen.org/en/digital-library/publications/2020/09/gender-equality-in-the-wake-of-covid-19.

UN Women. 2020b. "Violence against Women and Girls: The Shadow Pandemic." Statement by Phumzile Mlambo-Ngcuka, Executive Director of UN Women. https://www.unwomen.org/en/news/stories/2020/4/statement-ed-phumzile-violence-against-women-during-pandemic.

UN Women. 2020c. "Online and ICT-Facilitated Violence against Women and Girls during COVID-19." EVAW VOID-19 Brief. https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2020/Brief-Online-and-ICT-facilitated-violence-against-women-and-girls-during-COVID-19-en.pdf.

Vogels, E. A. 2021. "The State of Online Harassment." Pew Research Center.

West, J. 2014. *Cyber-Violence against Women*. Prepared for Battered Women's Support Services. http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf.

WHO (World Health Organization). 2021. "Violence against Women." Fact Sheet. https://www.who.int/news-room/fact-sheets/detail/violence-against-women.

Zhu, C., S. Huang, R. Evans, and W. Zhang. 2021. "Cyberbullying among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures." *Frontiers Public Health*, March 11, 2021. 9: 634909. doi: 10.3389/fpubh.2021.634909.