INTERSECTIONAL FEMINIST PERSPECTIVES ON CYBERCRIME LAW

Toward an effective and human rights-respecting implementation of the United Nations Cybercrime Convention

PEACE & SECURITY

CFFP THE CENTRE FOR FEMINIST FOREIGN POLICY

HEINRICH BÖLL STIFTUNG

Imprint
Authors: Centre for Feminist Foreign Policy (Vivienne Kobel), Pavlina Pavlova
Editor: Summer Banks
Design: Centre for Feminist Foreign Policy (Stefanie Hochkeppel)

February 2025

This policy briefing builds upon an eight-month project implemented between April and December 2024 by the Centre for Feminist Foreign Policy (CFFP) and funded by the Heinrich Böll Foundation.

Acknowledgements
We would like to thank the experts working at the intersection of cybersecurity, rule of law, human rights and gender for generously contributing their views to this report. Our special acknowledgement goes to Paloma Castro (Derechos Digitales), Veronica Ferrari (Association for Progressive Communications), Angela Minayo (Article 19 Eastern Africa), and 'Gbenga Sesan (Paradigm Initiative), for providing their expertise and sharing experiences that informed this policy brief. We are deeply grateful to feminist civil society, human rights and media freedom organisations, journalists, frontline defenders and all those tirelessly working to protect and advance human rights in the digital domain, often under very difficult circumstances. Without their vital work, this report would not have been possible.

Suggested Citation: CFFP and Pavlova (2025): Feminist Perspectives on Cybercrime Law - Toward an effective and human rights-respecting implementation of the United Nations Cybercrime Convention.

Email: hello@centreforffp.org

TABLE OF CONTENTS

Content warning: This policy briefing covers cases of sexual and gender-based violence and other forms of discrimination on the basis of gender and other (intersecting) identity markers.

List of Abbreviations

AHC	United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes
AI	Artificial Intelligence
CSAM	Child Sexual Abuse Material
CSO	Civil Society Organisation
CVSU	Cyber Victim Support Units
ECHR	European Court of Human Rights
EU	European Union
FOC	Freedom Online Coalition
ICT	Information and Communications Technology
NCSII	Non-Consensual Sharing of Intimate Images
NCIID	Non-Consensual Intimate Image Distribution
OHCHR	Office of the United Nations High Commissioner for Human Rights
TFGBV	Technology-Facilitated Gender-Based Violence
UNGA	United Nations General Assembly
UNODC	United Nations Office on Drugs and Crime

EXECUTIVE SUMMARY

As the global digital landscape evolves, cybercrime does not merely disrupt technological systems; it exacerbates pre-existing social and systemic inequalities and patriarchal structures, increasingly impacting the well-being of individuals and societies. Women, LGBTQIA+ individuals, journalists, human rights defenders and other groups who have been politically and/or historically marginalised on the basis of their gender, race, sexuality or other (intersecting) identity markers are impacted in a differentiated and often disproportionate manner. Starting from the fact that it is usually the same groups that are most vulnerable to cybercrime who have also been the targets of state overreach through weaponised cybercrime laws, this policy briefing highlights that national and international cybercrime legislation need careful scrutiny from an intersectional feminist perspective to prevent potential misuse.

The multi-stakeholder community has vigorously expressed similar concerns throughout the negotiations that led to the adoption of the United Nations Convention against Cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes (hereafter: UN Cybercrime Convention). While intended to address the challenges of transnational cybercrime, the UN Cybercrime Convention has drawn criticism for its potential risks, particularly the treaty's broad scope which could enable state overreach and thus compromise (digital) human rights and freedoms. Against this background, this briefing aims to contribute to paving ways towards a human-rights respecting implementation of the UN Cybercrime Convention, informed by intersectional feminist approaches.

First, it examines the differentiated and gendered impacts of cybercrime on marginalized individuals and communities, emphasising the necessity of an intersectional feminist approach (Chapter 2 and 3). Second, it assesses how national cybercrime laws have been weaponised by states to restrict (digital) human rights and freedoms, suppress dissent, and advance authoritarian and anti-feminist agendas (Chapter 4). Building on the lessons learnt from the national contexts, it evaluates the UN Cybercrime Convention through a gender-responsive and human rights-centred lens (Chapter 5), identifying both key risks and opportunities.

Findings:

- The UN Cybercrime Convention includes language in chapters on gender mainstreaming and emphasises the importance of addressing online gender-based violence.
- However, the treaty falls short of incorporating broader gender-sensitive and -responsive approaches and ensuring active promotion of gender equality across its provisions.
- The expansive scope of the UN Cybercrime Convention, particularly on international cooperation to share electronic evidence and on procedural powers,, risks turning the future UN instrument into a general data access treaty. Potential human rights violations include the targeting of marginalised groups and people in positions of vulnerability, due to inadequate human rights and privacy safeguards.
- The treaty's broad mutual legal assistance provisions risk enabling authoritarian states to misuse international cooperation for suppressive investigations, weakening safeguards against state overreach, and secretive data collection.

- The treaty's allowance for future protocols may open the door for an inclusion of content-related offences, such as extremism and terrorism-related offences, or the dissemination of false information. These highly subjective terms often serve authoritarian states to justify repressive measures and violations of the freedom of speech.

- The UN Cybercrime Convention extends to combating child sexual abuse material (CSAM). The fight against CSAM is paramount, especially given its long-term devastating effects on the victims and the prevalence of this crime. However, these provisions risk unintended consequences, including the potential criminalisation of minors for self-generated explicit content.

- The inclusion of non-consensual dissemination of intimate images (NCIID) marks a significant step toward addressing online gender-based violence, strengthening international efforts to prevent, investigate, and prosecute image-based abuse, while also encouraging strengthened cooperation among governments, online platforms, and civil society to protect victims and hold perpetrators accountable.

- While the UN Cybercrime Convention acknowledges the need for victim and witness protection, these articles defer to domestic laws that may lack effective safeguards, leaving victims, particularly those who may already face barriers in accessing justice, without legal guarantees for support, protection, or recourse.

- The impact of the UN Cybercrime Convention will depend on countries implementing the future instrument and how they translate its provisions into national frameworks. The treaty will shape national cybercrime laws, law enforcement measures, procedural powers, and international cooperation to prevent and combat cybercrime globally.

- Civil society and human rights organisations must actively monitor and provide feedback on the implementation and help ensure that the process and its outcomes are transparent, inclusive, and human rights-respecting.

To ensure that cybercrime law, especially in light of the UN Cybercrime Convention, adheres to human rights law, serves to protect marginalised communities and individuals in position of vulnerability, and promotes open, free, and just digital societies, this briefing proposes following **key recommendations** for states (details see p. 44-49):

1. Actively include and engage with the multistakeholder community in discussions and consultations on the decision to sign and ratify the UN Cybercrime Convention and, if applicable, in discussions on the future implementation of the treaty.

2. (Re-)Consider if signing the UN Cybercrime Convention is compatible with commitments to human rights and fundamental freedoms or other (political) commitments.

3. Commit to established human rights principles and safeguards in the implementation of the UN Cybercrime Convention and closely monitor the rights-respecting implementation of the treaty, including through adequate, effective and inclusive review mechanisms and other human-rights promoting measures, in cooperation with the multistakeholder community.

4. Promote an intersectional feminist approach to cybercrime legislation in (future) national and international norm-setting processes and discussion fora, particularly at the Conference of States Parties to the UN Cybercrime Convention (given it enters into force).

5. When implementing the UN Cybercrime Convention at a national level and designing/adapting national cybercrime legislation (accordingly), gender-mainstream cybercrime legislation and regularly carry out impact assessments according to intersectional feminist principles and in cooperation with (feminist) civil society and the multistakeholder community.

6. Promote and financially support capacity building, access to justice and gender-sensitive, victim-centred support for victims and survivors of cybercrime and state overreach.

7. Support independent interdisciplinary academic research, especially feminist scholars, and (feminist) civil society's work on cybercrime and cybercrime legislation.

1. INTRODUCTION

As stated in the Preamble of the United Nations Convention against Cybercrime, "information and communications technologies, while having enormous potential for the development of societies, create new opportunities for perpetrators, may contribute to the increase in the rate and diversity of criminal activities, and may have an adverse impact on States [and societies]" (United Nations General Assembly 2024a).

With the growing reliance on digital technologies, **cybercrime is increasingly impacting the well-being of individuals and societies**. While anyone can be impacted by cybercrime, **not everyone is affected equally**: individuals, communities, and groups who have been politically and/or historically marginalised on the basis of their gender, race, sexuality, socio-economic status, etc. are impacted in a differentiated and often disproportionate manner. Furthermore, cybercrime legislation **can be misused, serving repressive and often anti-feminist agendas**. Under the pretext of tackling cybercrime, authoritarian countries and those experiencing democratic backsliding have **weaponised cybercrime laws to undermine human rights, stifle dissent, and silence critical reporting**. Often the same groups that are most vulnerable to cybercrime are also the targets of state overreach through cybercrime legislation. This twofold harm hinders their ability to exercise their human rights and freedoms and to participate in society and political processes on equal footing with wider repercussions for democracy.

These and other human-rights considerations arose during the negotiations of the **United Nations Convention against Cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes** (short: UN Cybercrime Convention).[1] The first UN instrument on cybercrime acknowledges in its preamble "that the use of information and communications technology systems can have a considerable impact on the scale, speed and scope of criminal offences" (United Nations General Assembly 2024a) and recognises "the increasing number of victims of cybercrime, the importance of obtaining justice for those victims and the necessity to address the needs of persons in vulnerable situations in measures taken to prevent and combat the [cybercrime] offences" (ibid.). It further aims at "fostering international cooperation to prevent and combat such activities more effectively at the national, regional and international levels" (ibid.). Throuhout the negotiations, human rights organisations, civil society, the private sector, academia, and the technical community, alongside a number of states, emphasised the fact that the proposed text was deeply flawed due to its overbroad scope of criminalisation, amongst other aspects. Despite many objections[2], the UN Cybercrime Convention was adopted by consensus in the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC) on 8 August 2024 and approved by the UN General Assembly (UNGA) on 24 December 2024 (UN News 2024).

Building on the aforementioned concerns raised by many civil society organisations inclu-

ding CFFP, we now acknowledge the need to discuss and pave ways towards a human-rights respecting implementation of the UN Cybercrime Convention, informed by intersectional feminist approaches and principles. This policy briefing is an initial step in this process. It presents a three-stage analysis: first, it analyses the gendered and societal impacts of cybercrime, then explores how national cybercrime laws have been misused, in order to draw lessons and recommendations for future national cybercrime legislation, and the implementation of the UN Cybercrime Convention in particular. Concretely, the report

- explores the **gendered and societal impacts of cybercrime** on vulnerable, targeted, and marginalised individuals and groups to clarify why intersectional feminist cybercrime legislation is needed (Chapter 2),
- presents the **main elements of an intersectional feminist perspective on cybercrime legislation** (Chapter 3),
- analyses the **risks associated with national cybercrime legislation and assesses the role of anti-feminist and authoritarian actors** (Chapter 4),
- **examines the UN Cybercrime Convention** through feminist and gender-responsive approaches in order to assess potential risks and opportunities (Chapter 5),
- and proposes **actionable recommendations** for a human-rights respecting implementation of the UN Cybercrime Convention and for national cybercrime legislation to be designed and implemented in a gender-sensitive manner that respects human rights (Chapter 6).

This briefing discusses various kinds of harm caused by cybercrime and national cybercrime legislation. Wherever possible, the analyses and findings are illustrated by one or several cexamples from different countries. The examples presented are not exhaustive and merely serve as a representative snapshot. The choice of these cases does not imply any geographical preference (and/or other biases).

While this policy brief looks at the impact of cybercrime laws, and the misuse of these laws by (mainly authoritarian and democratically backsliding) states, it is important to note that this policy briefing is launched against the backdrop of an alarming deterioration of respect for human rights online and offline (Amnesty International 2024a) and declining global internet freedom (Freedom House 2024) – in both authoritarian and democratic countries. It is to be expected that the ongoing trends of polarisation, democratic backsliding and autocratisation (Nord et al. 2024), in combination with advances in technology, will further aggravate the impact of both cybercrime and oppressive/misused national cybercrime legislation on individuals – especially on those most marginalised – as well as on democratic structures and the universal human rights framework.

[1]The full text is annexed to the UN General Assembly Resolution A/RES/79/243 and accessible here: n2442674.pdf.
[2] See e.g. the following statements urging UN member states to reject the UN Cybercrime Convention in the UNGA and/or not to ratify it: 29 non-governmental organisations wrote a joint letter to the EU; the consortium of civil society organisations and academia, Al Sur, wrote an open letter to Latin American states; the Freedom Online Coalition's (FOC) Advisory Council proactively advised the FOC member states; and the International Chamber of Commerce issued a statement to governments.

2.THE DIFFERENTIATED IMPACTS OF CYBERCRIME AND CYBERCRIME LAW

Before summarising the differentiated impacts of cybercrime and cybercrime law, which will then be used as the basis for the development of an intersectional feminist approach to cybercrime legislation in Chapter 3, some terms and expressions will be clarified. More details on matters of definition are provided in the respective info boxes.

Defining Cybercrime

There is no single internationally recognised definition of cybercrime. Indeed, "the politics around the boundaries of the concept [of cybercrime]" (Hansel and Silomon, 2023: 9) have played an important role in efforts to establish cybercrime legislation at both the national and international level. In this policy briefing, if not otherwise noted, we are using a broad definition of cybercrime and examine country contexts that refer to both "cyber-dependent" and "cyber-enabled" crimes (including "content-related offences", see Chapter 4) as well as the justification, development and implementation of domestic and international legislative measures. A narrower definition would not prove useful, in particular from an intersectional feminist perspective, because "gendered cyber harms straddle standard distinctions between cyber-dependent and cyber-enabled threats and risks in the cybersecurity community" (Shires, Hassib & Swali 2024: 8).

INFOBOX 1

A BRIEF OVERVIEW OF CYBERCRIME DEFINITIONS

Out of the over 160 countries that have adopted legislation regarding cybercrime (UNODC, n.d.), some use the narrow definition of **"cyber-dependent" crimes** which rely entirely on computers, networks or other digital technologies (i.e., crimes such as unauthorised access to systems, spreading ransomware or Denial of Service (DoS) attacks, all of which would not exist without cyber technology). Broader definitions also include **"cyber-enabled" crimes**, i.e., "traditional" crimes that use digital technologies to enhance their scope, scale or efficiency but are not completely dependent on their digital dimensions, including cyber-enabled fraud, cyber stalking and harassment. A third type of cybercrime, which some states have subsumed under "cyber-enabled" crimes, are the so-called **"content-related offences"**. They revolve around the creation, distribution or hosting of illegal or harmful content in online space (e.g. on digital platforms) and include, depending on the country, the sharing of child sexual abuse material (CSAM), the non-consensual sharing of intimate images (NCSII), the dissemination of hate speech or incitement to terrorism online, and "insulting or defaming religion or religious values, threatening public morals and publishing fake news" (Hakmeh & Saunders 2024).[3]

[3] This info box is based on McGuire and Dowling 2013, UNODC-Education for Justice n.d. and Sarre et al. 2018. For a detailed review of different understandings and types of cybercrime and their digital evidence, see Kävrestad et al. 2024. A literature review and examples of cyber-dependent crimes, in particular, can be found in Maimon and Louderback 2019.

The cyber domain is an extension of the offline world and, in many respects, online space reinforces existing power imbalances, biases, discriminatory behaviours and abusive structures (see Bernarding & Kobel 2023). The harm caused by cybercrime can intersect with misogyny and patriarchal structures. Gender[4] and intersecting identities, including race, sexuality, socio-economic status and profession, thus play pivotal roles in determining the nature, form, severity and longevity of the inflicted harm.

INFOBOX 2

THE INTERSECTIONAL AND CONTEXTUAL NATURE OF (GENDERED) CYBER HARM AND ITS CASCADING AND COMPOUNDING EFFECTS

In addition to being **intersectional**, gendered cyber harm is **contextual**. As Pavlova (2024) points out, "policy and legal frameworks, gender norms and roles imposed by society and the state, access to services, social and family structures, and the environment [...] further influence the type, likelihood, and intensity of harm". Another mechanism amplifying gendered cyber-related harm is the interaction between different types of harm, described by Shires, Hassib & Swali (2024) in terms of hate speech, data breach and state overreach. The latter designates gendered cyber harm stemming "from states' use of policy and legislation to advance and enforce certain state-aligned gender norms online" (ibid.) by criminalising online content in cybercrime laws on the basis of gendered social norms or "morals" (Shires, Hassib & Swali 2024: 15). The Chatham House researchers examine what they call a **cascading and compounding effect**: one form of gendered cyber harm causes or is interconnected with another in a kind of cycle of harm, and these cascades increase the impact on those affected (ibid.).

[4] This briefing defines gender as a social construct that exists on a spectrum (i.e., it is non-binary) and is influenced by politics, the media, family structures, religion, laws, etc. Gender is a set of ideas that has an effect on socially expected, accepted, and rewarded behaviour and societal norms. It hierarchically structures our positions and roles in society as a way to maintain power hierarchies and structures of inequality among people, communities and states (CFFP Glossary 2021). Also, our understanding of gender in this briefing (and beyond) should never be equated with "women" only; it always includes men as well as all other persons.

Of the estimated 2.6 billion people currently offline (International Telecommunication Union 2023), the majority deprived of Internet access and use are women and girls (International Telecommunication Union 2024: 3).[5] Consequently, they have fewer paths to digital literacy, fuelling the digital divide which is one of the sources of increased vulnerability to cybercrime. At the same time, men have been found to be more likely to commit cybercrime, including offenses of a gender-based nature, such as the use of stalking malware against intimate partners (Bada et al. 2021). Women and girls, on the other hand, are particularly vulnerable to these crimes, especially when committed by partners or family members as a form of control and an extension of family violence and intimate partner abuse.

Control and manipulation of information, impersonation and identity theft, discriminatory speech, unauthorised/controlling access, threats, disparagement, non-consensual sharing of private information, technology-related sexual abuse and exploitation, attacks on communications channels, omissions by regulatory actors, harassment, extortion and surveillance and stalking are all forms of technology-facilitated gender-based violence (TFGBV)[6] that disproportionately affects women and has been enabled and amplified by the use of digital tools (United Nations Human Rights Council 2018; UNRIC 2024). Online harassment, image-based abuse, cyberstalking and other types of gendered cybercrime have been growing, notably expanding during the Covid-19 pandemic and more recently with the proliferation of commercialised AI tools (Uhlich et al. 2024; UNRIC 2024). Whether and at what threshold some forms of TFGBV, e.g., online harassment, can be prosecuted depends on national legislation. Nevertheless, various forms of TFGBV can intersect, i.e. harm caused by criminalised forms can be exacerbated by forms of TFGBV that are not (yet) criminalised.

It is important to note that not all women are affected by TFGBV to the same degree. Amnesty International's Troll Patrol study on online abuse against women politicians and journalists shows that, whereas, on average, all women in the study – no matter where they position themselves on the political spectrum – received an abusive or problematic tweet every 30 seconds, women of colour were 34% more likely to be targeted in such tweets than white women (Amnesty International 2018). Black women were even 84% more likely than white women to be targeted (ibid.). Also groups marginalised on the basis of other identity markers, such as their ethnic background and/or migrant status, have been increasingly affected by online hate speech (Democracy Reporting International 2023).

The impact on victims' lives, their families, children, jobs, relationships, and mental and physical health is considerable. Even though those affected by TFGBV are already paying a high price, and no figure can do justice to the individual suffering nor provide a remedy for it, it should be mentioned that an EU study estimates the overall costs of cyber harassment and cyber stalking of women at between 45 billion and almost 90 billion euro per year in healthcare costs, legal costs and labour market costs, among other financial impacts (Council of Europe 2021).

Gender considerations extend to the specific vulnerabilities of girls and boys, particularly

[5] Globally, 70% of men and 65% of women are using the Internet. On the international level, we are moving towards gender parity (score of 0.94 in 2024), with the exception of Least Developed Countries, where the gender parity score has decreased from 0.74 to 0.70 in 2024 (ibid.).

[6] The 13 manifestations of gender-based violence using technology are explained in detail here: https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology.

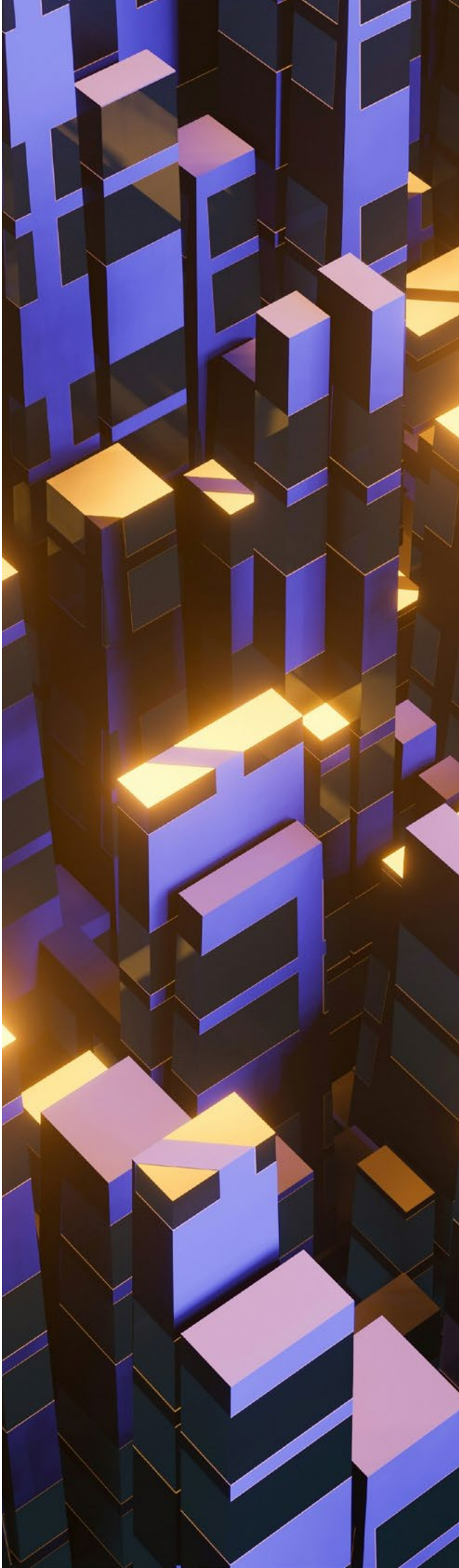
concerning child-sexual abuse material (CSAM) or "sextortion" schemes targeting minors. In Indiana (USA), e.g., law enforcement agencies have reported that at least 3,000 minors, primarily boys, became victims of online sextortion in 2023 (US Attorney's Office, Southern District of Indiana 2023). The non-consensual sharing of intimate images (NCSII), often dubbed "revenge porn" is a growing form of gendered cyber harm. With the introduction of commercialised AI generators, such sexualised explicit content (such as deepfake porn) can be easily created, without consent, and predominantly targets women and girls (StopNCII.org n.d.). While public data remain scarce, the Revenge Porn Helpline, which, the Revenge Porn Helpline, which supports victims of NCSII, documents caseloads increasing year-by-year and doubling in 2020 during the COVID-19 pandemic (SWGfL n.d.).

Finally, indiscriminate cybercrime which does not target specific individuals or groups can also have differentiated and severe impacts due to gender identity or expression. Gender can be a factor of vulnerability given the sensitivity of data or other context-dependent repercussions. For example, when hacked and leaked data includes personal medical information relating to sexual or reproductive health, rights, and history (e.g., abortions), these data leaks can threaten women and LGBTQIA+ communities more than others. This is because the information related to abortions or sexual preference can be used to further intimidate and ostracise targeted individuals, especially in countries where such conduct is illegal (Pavlova 2024).

An individual's identity, including even their occupation, plays an important role in determining how intensively they are targeted and how vulnerable they are to cybercrime. Journalists, whistle-blowers, human rights defenders, activists, dissidents, and political candidates have been exposed to online harassment, to sexualised online threats and intimidation, and to surveillance at higher rates (Amnesty International 2018; Pavlova 2024; UNESCO 2020). For example, the Pegasus Project, a collaboration between 17 media organisations investigating the use of the Israeli NSO Group's Pegasus spyware, revealed that at least 180 journalists in 20 countries were selected for potential targeting with the NSO spyware between 2016 and 2021 (Amnesty International 2021). This number, including various journalists in countries experiencing democratic backsliding and autocratisation, illustrates how spyware has been used to intimidate and silence critical media (ibid.). The NSO Group neither confirmed nor denied its government clients but rather claimed that the Pegasus Project made "incorrect assumptions" (ibid.). In other instances, states could be clearly identified as the perpetrator. For example, a 2018 investigation by the Israeli newspaper *Haaretz* uncovered the fac that the Indonesian government had acquired surveillance software to compile a database of LGBTQIA+ rights activists to target for surveillance (Pavlova 2024 with reference to Haaretz 2018). "[T]he mere presence - or even the perceived presence - of surveillance can result in psychological harm, privacy and security concerns, and a chilling effect. This often leads targets to withdraw from social or public life or alter their behavior to conform to imposed norms. Victims of intrusive surveillance report mental stress, paranoia, social isolation, and self-censorship for fear of a possible backlash" (Pavlova 2024).

Cybercrime law as a tool of state overreach

Criminal justice frameworks, if implemented in a human-rights-respecting manner, can and should provide justice and recourse to cybercrime victims, witnesses, and survivors. Cybercrime law can include provisions of assistance and protection to victims of criminal offences, including measures that assist their physical and psychological recovery. In many instances, however, cyber-related legislation has been misused to justify state overreach and support anti-feminist and patriarchal agendas. Authoritarian states and countries experiencing democratic backsliding, in particular, repurpose cybercrime law as a pretext to undermine individuals' rights and freedoms and criminalise those who fight for the rights of some of the most vulnerable members of society. For instance, cybercrime laws can be used to legitimise disproportionate censorship and surveillance measures and, in some cases, these harms can be exacerbated by discriminatory access to justice (see Chapter 4).



3. AN INTERSECTIONAL FEMINIST APPROACH TO CYBERCRIME LEGISLATION

The intersectional feminist approach to cybercrime legislation[7] goes beyond approaches that are based on human security, human rights and women's participation. It builds on the understanding that the intersection of identity markers, such as gender, sexuality, employment/profession, class, ethnicity and race, adds to the potential aggravated negative impacts of cybercrime and misused cybercrime legislation on historically and/or politically marginalised groups (see Chapter 2). These repercussions undermine and limit progress on gender equality, human security, and human rights for all.

Intersectional feminist approaches to cybercrime legislation focus on the intersectional gender-mainstreaming[8] of the design, implementation and evaluation of legal provisions on cybercrime. It further transcends mere (legislation-related) gender-mainstreaming efforts by including analyses of the national and global political and judicial systems and structures where cybercrime legislation is negotiated, established, implemented and evaluated. These approaches further acknowledge that people experience unequal effects on their (perception of) security and human rights from cybercrime, its online or offline repercussions, as well as the laws and judicial system by which the state tries to deter, mitigate and sanction cybercriminal activities (see Chapter 2).[9] They shed light on intended and/or unintended harms that can stem from provisions, accompanying safeguards and their practical implementation – especially considering how existing cybercrime legislation can be, and already is, weaponized against targeted, discriminated or marginalised groups (see Chapter 4).

Cybercrime legislation is neither designed nor enforced in a vacuum. The laws always reflect different cultural and/or contextual understandings of "cybercrime" (see Hu, Chen & Bose 2013). For this reason, the application can be influenced by often gendered, patriarchal social norms (or what authoritarian governments often efer to as "public morals"). Criminal justice provisions can be applied in a discriminatory or biased manner to

[7] This briefing acknowledges that countries often do not have one single cybercrime law as part of their criminal code but rather include legal provisions or political agendas concerning (different types of) cybercrime in cybersecurity strategies and laws and/or in legal acts covering media freedom, intellectual property rights, personal data protection, the misuse of computers, e-commerce, counter-terrorism measures and other cyber-related topics. UNODC's Database of Legislation contains a rich overview of different cybercrime-related regulatory efforts by UN Member states. It can be accessed here: Database of Legislation.

[8] Intersectional gender-mainstreaming assesses the gender implications of any policy and/or action, at all levels, while considering the effects of the same actions and/or policy on other identity markers such as race, class and ethnicity. It ensures that all concerns voiced by groups marginalised on the basis of gender or other identity markers, and their experiences and aspirations, are integral to the design, implementation, monitoring and evaluation of policies (especially of those that directly affect them). The ultimate goal of intersectional gender-mainstreaming is promoting gender equality, ensuring equal benefits for all, reducing inequality and facilitating progress toward sustainable development (Kataeva et al. 2024).

[9] Cybersecurity and cybercrime are related and intersecting issues. However, cybersecurity is a proactive and preventive concept and focuses on preventing threats and vulnerabilities in and through cyberspace, whereas talking about cybercrime means that cyber-related hostile acts and offences have already been committed. Cybercrime regulation is thus a rather reactive concept because it investigates and prosecutes malicious, often illegal acts.

criminalise activities based on the targeted person's gender (or other identity markers). At the same time, despite cybercrime having numerous gender-specific impacts (see Chapter 2), not all countries take gender (in)equality considerations adequately into account when designing, implementing and evaluating cybercrime legislation. Some countries have introduced new laws or revised existing ones criminalising at least some forms of Technology-Facilitated Gender-Based Violence (TFGBV)[10] , such as sextortion[11] or the non-consensual sharing of intimate images (NCSII, see Chapter 5). Nevertheless, an intersectional feminist perspective on cybercrime legislation emphasises the fact that, in order to prevent and mitigate harm inflicted on individuals, such laws need to be designed inclusively and in consideration of the lived experiences and needs of victims and survivors of (gendered) cybercrime.

An intersectional feminist perspective on cybercrime legislation also highlights the fact that intersecting identities play a considerable role in access to justice[12] and the right to due process and effective remedy (see also: Derechos Digitales & Association for Progressive Communications 2023). States' justice systems cannot be considered gender-neutral but rather they often reflect patriarchal and discriminatory norms and inequalities on the basis of gender or other (intersecting) identity markers.

Marginalised persons, including racial and ethnic minorities, the LGBTQIA+ community, disabled people and low-income groups often face barriers to accessing justice. This can be due to the mentioned systemic (gendered) biases within the legal system or other factors such as limited mobility, financial constraints, language skills or digital illiteracy (Creutzfeldt et al. 2024; Ghai & Cottrell 2009). And even if marginalised persons access the justice system, their testimonies and experienced harm may be downplayed or discredited. These groups also experience unfair or unlawful treatment or trials, potential intended or unintended re-victimisation and other forms of discrimination throughout their interactions with law enforcement and the wider justice system (Penal Reform International 2012).

Against this backdrop, feminist approaches to cybercrime legislation centre the lived experiences of survivors, victims and witnesses of cybercrime and those affected by the misuse of cybercrime legislation. They call for comprehensive, intersectional gender-sensitive/gender-responsive victim support, non-discrimination procedures and practices, and the minimisation of potential re-victimisation.

It should be noted that taking an intersectional feminist approach to cybercrime legislation in this briefing does, by no means, imply that women, LGBTQIA+ people, and other marginalised groups are vulnerable per se. Viewing them solely as victims disregards their agency, resilience, and roles in combating these harms and in actively creating and shaping safer and more inclusive

[10] The Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW Platform) provides a list of country examples in their report „The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform" (Council of Europe 2022).
[11] Sextortion, in comparison to other types of sexually abusive conduct, contains both a sexual as well as a corruption component. It thus involves a request to engage in sexual activity, and the perpetrator must occupy a position of authority or abuse their power in a kind of "this-for-that" exchange (International Association of Women Judges n.d.).
[12] Access to justice is a fundamental human right which guarantees that every individual can protect themselves from violations of their rights, seek and obtain remedies, and hold both private persons and the state accountable – "ensuring that legal and judicial outcomes are just and equitable" (Lima & Gomez 2021)

4. NATIONAL CYBERCRIME LEGISLATION AND STATE OVERREACH

With cybercrime legislation, as with any part of the criminal justice system, it is vital to ensure that the provisions are not applied in a way that violates but rather strengthens human rights. For this reason, safeguards for the protection of fundamental freedoms such as the freedom of expression, the right to privacy and other human rights, in particular those of marginalised individuals and groups, need to be included. However, in various parts of the world, cybercrime legislation is used as a legal tool to stifle dissent, restrict civic spaces and reinforce autocratic rule through the surveillance, silencing, and prosecution of women, LGBTQIA+ individuals, journalists, (feminist) human rights advocates and other critical voices – online and offline (Derechos Digitales & Association for Progressive Communications 2023; GenderIT.org 2008; Shires, Hassib & Swali 2024).

This not only has serious consequences for the targeted individuals' (perceived) freedom, security, and exercise of human rights but also further social and political impacts. For women, the LGBTQIA+ community and other marginalised groups who have been historically or politically excluded from meaningful political participation in the offline world, the Internet has played a key role in strengthening and expanding the exercise of their freedom of expression, association and peaceful assembly. For example, both Iranian and Afghan women have turned to social media platforms to organise protests, share their experiences under authoritarian rule and advocate for gender equality (RadioFreeEurope/RadioLiberty 2021), shifting "the scale of visibility for women's rights activism from a local stage to a global stage" (Koutchesfahani 2022) and ensuring international awareness despite severe restrictions on traditional media. Especially in contexts where women, LGBTQIA+ people and other marginalised groups face online or offline (gender-based) barriers to the freedom of expression and opinion, cybercrime laws can further aggravate the situation. Usually transferring disproportionate investigative powers to government authorities, domestic legal systems can facilitate or even legalise (gender-based) breaches of privacy and (gendered) data weaponization (see Chapter 4.2.). Just the fear of being targeted can lead to self-censorship or a loss of the free-

dom of expression (United Nations Human Rights Council 2020). Given the universality, indivisibility and interdependence of human rights, state-led attacks using cybercrime legislation to undermine freedom of expression and the right to privacy – particularly those targeting marginalised groups – must be seen as an assault on gender equality, the broader human rights framework, and as a threat to sustainable development, peace and democracy (United Nations General Assembly 2021; United Nations Human Rights Council 2020). There is a range of strategic, cross-contextual patterns by which states have unduly restricted the rights of women, LGBTQIA+ people and other marginalised groups. They manifest both in terms of the design of cybercrime legislation (definitions of terms and scope) and its implementation by law enforcement (access to justice, judicial process, possible remedies). Moreover, cybercrime laws often allow authorities to access and retain individuals' data under the guise of cybercrime investigation and allow misuse of surveillance technology (see Chapter 4.2.

Despite the different geographical and cultural contexts that the selected cases stem from, many laws and related (criminal/judicial) systems appear to be rooted in similar authoritarian playbooks. The latter are often interlinked with and permeated by anti-feminism, i.e., based on cultural values, beliefs and/or norms which are critical of gender (equality) and other feminist and human rights-related demands (Derechos Digitales & Association for Progressive Communications 2023: 9).[13] Some of the countries analysed also criminalise same-sex relations and/or reject gender (equality) per se.

It should be noted that this chapter is an analysis of the potential and actual pitfalls of (exemplarily chosen) national cybercrime laws and not an analysis of cybercrime legislation per se.

[13] Autocratisation and democratic backsliding are often deeply intertwined with anti-feminism. As the Centre for Feminist Foreign Policy's publication "Strongmen and Violence: Interlinkages of Anti-Feminism and Anti-Democratic Developments" highlights, anti-democratic and authoritarian actors "strategically use anti-feminist discourse and policies to consolidate power at domestic, regional, and international levels and to undermine the rule of law and other pillars of democracy" (Seitenova, Kobel & Bernarding 2024: 2). While the role and functions of anti-feminism are context-dependent, CFFP's report highlights two key mechanisms: firstly, anti-feminist narratives serve authoritarian actors by justifying the internal oppression of marginalised groups and secondly, they are instrumentalised to advance these actors' foreign policy strategy and/or to wage and justify conflicts (ibid.: 3).

4.1. THE NEED FOR CLEAR DEFINITIONS: EXPANSIVE SCOPES IN NATIONAL CYBERCRIME LAWS CAN LEAD TO UNINTENDED CONSEQUENCES

National cybercrime legislation often uses generic, vague and overly broad terms and is thus open to oppressive, arbitrary interpretation and weaponisation by governments (Human Rights Watch 2021). Many cybercrime laws extensively criminalise online speech on grounds such as spreading "fake/false news", "disinformation", "conspiracy", or "indecent content", threatening "national security" or "unity", and/or undermining "public morals" or "traditional values". The case studies below show how such vaguely defined terms are misused by states who actively ignore existing human rights safeguards and the principles of legality, necessity, proportionality and non-discrimination already in place to balance out restrictions on freedom of speech and to prevent state overreach.

Weaponising "public morals" and "family values" against women and LGBTQIA+ people and their free speech online

Both the gendered roots and impact of national cybercrime laws and/or judicial decisions are probably most visible when such laws cite the protection of "public morals" as a reason to criminalise online speech and remove content from the Internet. In many patriarchal societies where women's and other marginalised groups' gender identity, sexual expression, bodies and behaviour are devalued, judged and policed on the basis of (binary) gendered norms, their online audio, video or written self-expression is usually perceived and/or framed as "improper" or "obscene".[14] Authorities in these countries often claim that a restriction of women's freedom of expression online is needed to protect women and the society, the country's culture, and/or traditional family and moral values (see, e.g., Bhandari & Kovacs 2021). However, "[s]uch paternalistic approaches do not take women's consent into account and see any expression of female sexuality as problematic, transgressive and punishable" (United Nations General Assembly 2021).

The European Court of Human Rights (ECHR) and the UN Human Rights Committee (HRC) have ruled that invoking the broad concept of "public morals" alone does not sufficiently justify restrictions on the freedom of expression and opinion without more concrete and substantial justification (Mendel n.d.; United Nations Human Rights Committee 2011).[15] Furthermore, restrictions on the freedom of expression "for the purpose of protecting morals must

[14] We acknowledge that, in the large majority of societies, both in the Global North and in the Global South, patriarchal systems of power persist. This chapter should thus, by no means, imply that patriarchal systems and their detrimental effects on societies, particularly marginalised communities, were only an issue in countries outside of Europe/the Global North. Due to the scope and aim of this briefing, however, we only cover countries with recorded cases in which national cybercrime legislation was instrumentalised to discriminate against women and other marginalised groups.

[15] For example, according to Article 10 (2) of the European Convention on Human Rights, a restriction on freedom of expression must not only protect one of the overriding interests in Article 10 (2) and be prescribed by law, but also be "necessary in a democratic society" (Mendel n.d.).

be based on principles not deriving exclusively from a single tradition" (United Nations Human Rights Committee 2011: 8) and "be understood in the light of universality of human rights and the principle of non-discrimination" (ibid.). In the following exemplary cases in Egypt and Libya, however, these human rights standards are being deliberately ignored. The gendered abuse of national cybercrime laws sends an alarming signal about the state of (digital) women's rights and gender equality in these countries.

In Egypt, arrests of women on grounds of violations of "'morality' [...] have skyrocketed" under President Abdel Fattah al-Sisi, according to Human Rights Watch (cited in Makooi 2023). Indeed, in connection with the adoption of Egypt's *Law No. 175 on Anti-Cyber and Information Technology Crimes* in 2018[16] (hereafter: Cybercrime Law No. 175) and women raising their voices in the context of a #MeToo social media campaign in 2020, Egyptian authorities have deliberately targeted female social media influencers (Allinson 2020; Juma & Knipp 2020). In 2023, for example, they arrested and detained the model and TikTok personality Salma Elshimy on vague charges of inciting "debauchery" and "violating family values" through her social media posts which, according to Egyptian authorities, "contradict social morals and values" (Makooi 2023). In most of her content on TikTok, the influencer appears completely dressed and films herself while posing, dancing, or singing. Silencing and arresting women for merely peacefully sharing videos and photos about themselves online which are deemed "indecent" by the Egyptian government is discriminatory "and directly violates their right to free expression", as Human Rights Watch, which has highlighted at least 15 cases similar to Salma Elshimy's, rightly points out (Human Rights Watch 2020). In April 2023, Elshimy was sentenced to two years in prison and a fine of 100,000 Egyptian pounds (around 2,000 USD) by an Alexandrian court on the basis of the above-mentioned vague accusations, according to her lawyer (The New Arab 2023).

Egypt has long discriminated against the queer community and established "a complex legal infrastructure of interpretations and precedents [that] has allowed for continuous and targeted prosecution of LGBTQ individuals" (Rigot 2020). In recent years, cases involving LGBTQIA+ persons have been increasingly referred to economic courts which have jurisdiction over the 2018 Cybercrime Law No. 175, whose vague terms like "family values" lack interpretation from higher courts and thus enable "judicial power to not just apply these laws but also to define them", as Afsaneh Rigot, researcher at Article 19, underlines (ibid.). This not only creates legal uncertainty for the LGBTQIA+ community through a chilling effect on public online gender and sexual expression and free speech, but Egyptian tactics to criminalise LGBTQIA+ persons through ICT-related laws risk to be copied by other repressive governments (ibid.).

In February 2023, the Libyan Ministry of the Interior announced that they had arrested prominent singer Ahlam al-Yamani and content creator Haneen al-Abdali for "crimes violating public morals" under *Law No. 5 on Combating Cybercrime* of 2022[17]. Al-Yamani and al-Abdali are accused of "insulting the status of the chaste and dignified Libyan woman in our conservative society with acts and behaviors that are foreign to us and offend our customs, traditions and true religion" (cited in: Human Rights Watch 2023a). The law – highly criticised by United Nations experts and

[16] The full text can be found here: Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes, Egypt, WIPO Lex.

[17] The full text of the law can be found here: قانون رقم 5 لسنة 2022 م بشأن مكافحة الجرائم الإلكترونية - الموقع القانوني.

human rights advocates (United Nations Human Rights Council 2022) for its overbroad definitions, the risk it presents of prosecution for peaceful expression and its prison terms of up to 15 years for violators – was adopted without consulting civil society or tech experts and does not further define "public morals" (Human Rights Watch 2023a; Africanews 2023). There have been no available updates on the case to date.

Criminalising online criticism against the government through accusations of "fake news", "defamation" or attempts at "undermining national security"

In addition to "public morals", repressive governments have also increasingly established crimes related to vague terms such as the "propagation of fake/false news", "defamation" or online expression and content "undermining national security". The exemplary case studies of Nicaragua, Tunisia and Jordan demonstrate how this has serious effects on the freedom of expression of human rights advocates, journalists, and other critical voices – those who raise awareness of repressive practices and protect the rights of the most marginalised individuals and vulnerable groups in society.

According to the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, laws adopted to tackle disinformation, sometimes called "fake news" laws, are often misused to stifle dissent (2021: 18). Nicaragua's *Special Law on Cybercrime* (hereafter: Special Law), in force since 2020 and dubbed the "gag law", is just one daunting example illustrating this issue. It led to the prosecution and arrest of various Nicaraguan political opponents and journalists for allegedly spreading disinformation (Stock 2021). According to a report by Derechos Digitales, Article 30 of the Special Law prohibits the propagation of "false news" without defining what is considered as such (2023). For example, it does not differentiate between "when a person intends to share a news item with harmful motives and when it was a mistake" (ibid.). The Special Law establishes prison terms of two to four years for "those who promote or distribute false or misleading information that causes alarm, terror, or unease in the public" (AP News 2020). If the information "incites hatred or violence, or puts at risk economic stability, public health, national sovereignty or law and order", sentences increase to three to five years in prison (ibid.). The Nicaraguan Special Law was misused to silence medical personnel expressing criticism about the management of the Covid-19 pandemic (Derechos Digitales 2023), as well as against a number of activists, including frontline defenders. For example, in September 2021, Amaru Ruiz Alemán, an indigenous rights defender in exile, was charged with "propagation of false news through information and communication technologies" in connection with his social media activities denouncing violations of indigenous peoples' human rights in Nicaragua, including a massacre against indigenous and land rights defenders in the Mayangna Territory (ProtectDefenders.eu 2021; OMCT 2021). Faced with the risk of being prosecuted under the Special Law, many journalists and traditional media outlets – those who have not stopped reporting out of (legitimate) fear – have gone into exile or created new digital media platforms or social media accounts, sometimes under pseudonyms, to continue reporting (Derechos Digitales 2023). However, the Special Law's chilling effect on critical journalism and speech might be worsened due to a recent reform, ordered by President Daniel Ortega in September 2024. Now, the Special Law can be applied not only to crimes committed "through information technology" but also to "the use of social networks and cell phone applications" (Miranda Aburto 2024). Moreover, the reform increased the above-mentioned prison sentences to five to ten

years, respectively (ibid.). These amendments are part of a package of reforms that is seen amongst legal and human rights experts as "an attempt to 'legitimise' the persecution of critics of President Daniel Ortega, both inside and outside the country" (AFP 2024).

In Tunisia, in October 2024, the TV commentator Sonia Dahmani was found guilty and sentenced to two years in prison under Article 24 of the draconian *Decree-Law No. 2022-54 of 13 September 2022 on combating offences relating to information and communication systems*[18] (hereafter: Decree-Law No. 54), on the basis of remarks she made about Tunisia's treatment of migrants from sub-Saharan Africa. The Tunisian cybercrime statute criminalises activities that "produce, spread, disseminate, send or write false news [...] with the aim of infringing the rights of others, harming public safety or national defence or sowing terror among the population" (AP News 2024) and, if invoked, can lead to imprisonment for five years and a fine of 50,000 dinars (about 15,000 USD). Dahmani is being prosecuted in four other cases under the same Decree-Law 54 for statements she made earlier on, for example, racism against Black migrants in Tunisia (La Presse 2024). She is not the only one affected by President Kais Saied's tool to silence his critics – two of her colleagues were also sentenced to one year in prison under the same Law. In 2023, Human Rights Watch documented how Decree-Law 54 was instrumentalised to sentence two political opposition activists to prison terms for criticising Saied's government and "to detain, charge, or place under investigation at least 20 journalists, lawyers, students, and other critics for their public statements online or in the media" (Human Rights Watch 2023b). Against this backdrop, media freedom and human rights advocates have described Decree-Law 54 as "symptomatic" of Saied's authoritarian strategy for limiting the freedom of expression (and breaching international standards on freedom of expression) in order to undermine democratic institutions in Tunisia under the guise of protecting "national security" (Boutry 2024; Benshimon 2024, ibid.).

Restricting the rights to freedom of expression, association and peaceful assembly, and to protest[19]

Jordan's new *Law No. 17* of 2023 on combating cybercrimes (hereafter: Law No. 17)[20] reads like the two cases above. It extends the scope of the offences of the 2015 Law No. 27 on cybercrime and law enforcement powers and introduces harsher prison sentences of a minimum of three months and fines up to 32,000 JOD (about 45,000 USD). It uses imprecise, undefined language which does not comply with international law standards. Moreover, it criminalises the publication and circulation of content, including information deemed to be "fake" and "slander" by the government, and introduces higher penalties for other vaguely defined offences such as "threatening societal peace", "contempt for religions", "provoking strife" and "online assassination of personality" (Jbour 2023; Amnesty International 2024b)[21]. Since it entered into force in 2023, the law has been wea-

[18] The full text of the law can be found here: Décret-loi n° 2022-54 du 13 septembre 2022, relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication - Tunisie - Legal Databases. A legal analysis reviewing the Decree-Law No. 54's compliance with international human rights and freedom of expression standards by the organisation Article 19 can be found here: Analysis-of-decree-law-54-English.pdf .

[19] Civicus has tracked a large number of cases in which the Jordanian cybercrime law was used to target protesters, human rights defenders and journalists in relation to the pro-Palestinian protest and (connected) online content: Draconian Cybercrime law used to target protesters, HRDs, journalists amid pro-Palestine protests - Civicus Monitor.

[20] The full text can be accessed here: https://perma.cc/7RSM-6S4K.

4.1.THE NEED FOR CLEAR DEFINITIONS: EXPANSIVE SCOPES IN NATIONAL CYBERCRIME LAWS CAN LEAD TO UNINTENDED CONSEQUENCES

ponised by the Jordanian government "to harass, punish and intimidate those expressing opinions that are critical of the authorities amid an escalating assault on the rights to freedom of expression, association and peaceful assembly in the country" (Amnesty International 2024c). After the Hamas terrorist attack on 7 October 2023, and the subsequent military response by Israel, hundreds of activists, journalists, politicians and Internet users who expressed solidarity with Palestine through posts or videos, criticised Jordan's policies towards Israel (including Jordan's peace deal with Israel) or called for peaceful protests on social media have been prosecuted and/or questioned under Law No. 17 (ibid.; Amnesty International 2024b). The two following cases evidenced by Amnesty International illustrate this situation.

> "Journalist Hiba Abu Taha is currently serving a one-year sentence in al-Juwaida Correction and Rehabilitation Centre in the south of Amman over an article she wrote in which she criticised Jordan's interception of Iranian missiles headed to Israel in April 2024. A criminal court convicted her on 11 June 2024 of using social media platforms to 'spread false news, or insult or defame a governmental authority or official body', and for 'inciting strife or sedition or threatening societal peace or inciting hatred or violence' (Amnesty International 2024b).

In the second case, activist Fatima Shubeilat was arrested at a shopping mall in Amman after a video showing her participation in a pro-Palestinian protest in Amman circulated on social media.

> "According to her lawyer, she was initially charged with 'unlawful gathering', 'resisting security personnel' and 'insulting a public official' under [...] the Penal Code. The public prosecutor initially agreed to release her on bail but then reneged, saying that the Cybercrimes Unit had initiated another separate case against her under articles 15 [on spreading fake news or defamation] and 17 [on sedition or strife] of the Cybercrimes Law. She was released on bail on 30 April, and her trial for both cases is still pending (ibid.).

[21] The restrictions and violations of the freedom of expression in the context of (online and offline) pro-Palestinian protest and solidarity in Jordan need to be contextualised as part of a larger development. "The conflict in Gaza has unleashed a global crisis of freedom of expression" (UN General Assembly 2024b) not only in authoritarian but also in democratic countries (ibid.). As the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, states in her 2024 report, media freedom has been curtailed and pro-Palestinian protest, and dissent has been censored and suppressed offline and/or online (2024: 7f, 10), with antisemitic and anti-Muslim hate speech and online harassment surging at the same time (New York Times 2023; BBC 2024). As the "extensive pattern of unlawful, discriminatory and disproportionate restrictions and repression of freedom of expression, primarily of Palestinian activists and their supporters in Western Europe and North America" (UN General Assembly, 2024: 19) is mostly not based on cybercrime law(s), it is not part of this policy brief's analysis.

About the calculated (gendered) "side-effects" of targeting critical voices in the guise of accusations of cybercrime

In other instances, the prosecution of (marginalised) individuals for using criminalised speech serves governments not only by stifling any kind of online criticism against them, but also by helping them to achieve certain repressive (gendered) "side-effects" beneficial to their authoritarian and often anti-feminist agendas.

This becomes evident in the case of researcher Dr. Stella Nyanzi from Uganda. In 2017, Nyanzi, an outspoken feminist and critic of President Yoweri Museveni's government, was charged under Uganda's 2011 *Computer Misuse Act*[22] for "offensive communication" and "cyber harassment" of Museveni (The Independent 2023; Columbia University n.d.). She had been arrested for calling Musevini "a pair of buttocks" in a Facebook post and for a few earlier posts. However, evidence suggests that the instance of Nyanzi raising her voice online against the authorities was not the only reason for her being targeted under the Computer Misuse Act. In the same year, Nyanzi had launched the #padsforgirlsUG campaign in response to Musevini's broken promise to support the education of girls by providing sanitary pads in schools. Over the course of this campaign, she was arrested and also lost her job at the Makerere University after she participated in a Twitter argument on the topic with the president's wife (Human Rights Foundation 2017; Mwesigwa 2017).

Uganda has an alarming record of gender-based discrimination and violence, with LBGTQIA+ organisations being banned and oppressive, radical anti-gender laws criminalising consensual same-sex conduct and imposing the death penalty in certain circumstances (Human Rights Watch 2024a). Against this backdrop, Nyanzi's prosecution – not only as a government critic, but also or especially as a women's rights and LGBTQIA+ activist – was analysed by human rights experts such as Maria Burnett from Human Rights Watch as a gendered attempt to hit two birds with one stone, "[the government was] seeking to intimidate and terrify her and her family and her community of supporters who are largely from Uganda's human rights, women's and LGBT movement" (Slawson 2017, cited in Derechos Digitales & Association for Progressive Communications 2023). This assessment is underlined by a statement from a government spokesperson who was interviewed during the proceedings against Nyanzi and reportedly said, "I doubt Nyanzi or the forces behind her, which is Besigye and company plus the LGBT lobby, can sustain an extended political fight with us Government on any issue" (cited in: Columbia University n.d.).

[22] The full text can be accessed here: ug-act-2011-2-publication-document.pdf.

4.2. THE NEED TO PROTECT DIGITAL (CIVIC AND PUBLIC) SPACES AND PRIVACY: STATE SURVEILLANCE ON THE BASIS OF NATIONAL CYBERCRIME LEGISLATION AND ITS SILENCING EFFECTS

As the 2019 "Surveillance and human rights" report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression states, "[p]rivacy and expression are intertwined in the digital age, with online privacy serving as a gateway to secure exercise of the freedom of opinion and expression" (United Nations Human Rights Council 2019a: 8). International human rights law contains established principles to clarify when interference with the right to privacy is permitted (see ibid.: 7f, III. A. 24.) and the General Assembly Resolution 73/179, echoing these principles, stipulates that "surveillance of digital communications [...] must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory" (United Nations Human Rights Council 2019a: 8f). If these principles are not upheld, targeted surveillance can lead to self-censorship, chilling critical reporting and undermining "the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information" (United Nations Human Rights Council 2019a: 9) with catastrophic consequences for democracy and the protection of the human rights framework.

The following examples underline the risks and actual harm caused by national cybercrime legislation that enables (mass and/or targeted) state surveillance.

In the case of the 2022 Libyan Anti-Cybercrime Law (hereafter: the Law), UN experts[23] had expressed serious concerns that it "could have a grave impact on the enjoyment of the right to freedom of opinion and expression and the right to privacy" (United Nations Human Rights Council 2022: 1) and encouraged a withdrawal of the Law. According to the UN experts' commentary that was issued in March 2022, half a year before the Libyan House of Representatives passed the Law, it "would grant the Libyan authorities far-reaching powers to conduct mass surveillance of individuals using the internet or digital technologies" (ibid.: 8). In terms of risks of mass state surveillance, it was Article 7 of the Law in particular that was criticised in the commentary, as well as by civil society experts (Human Rights Watch 2023a). It allows for the governmental National Information and Security and Safety Authority (NISSA) to monitor the information and content made available, disseminated or displayed on/through the Internet or any other technologies

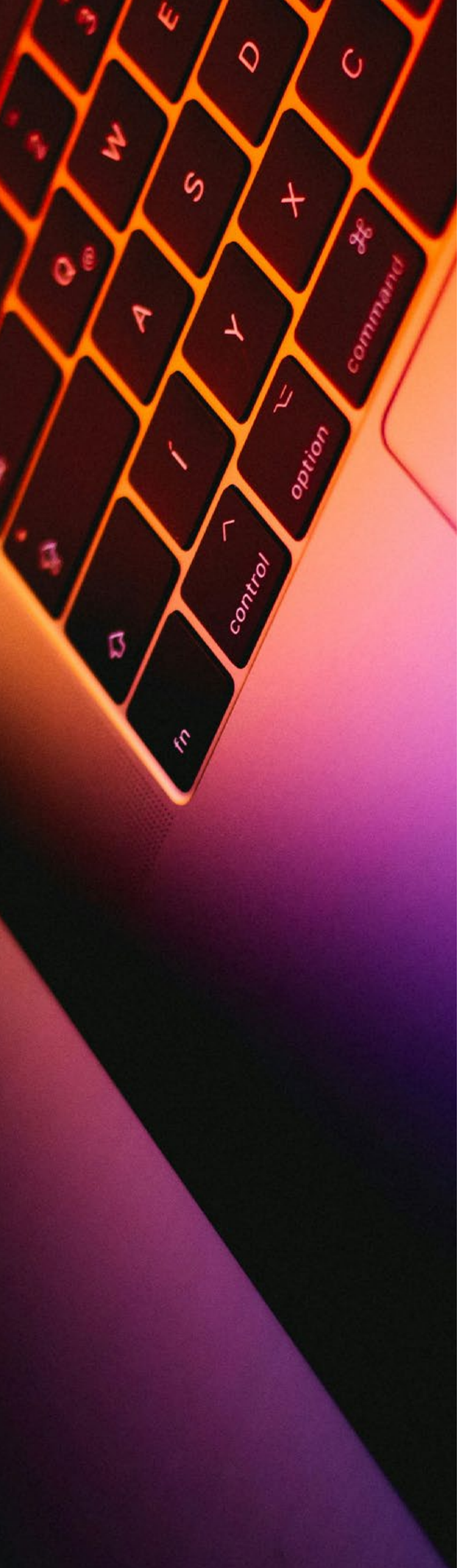
[23] The commentary was written by the Special Rapporteurs on the promotion and protection of the right to freedom of opinion and expression (Irene Khan), the Special Rapporteur on the rights to freedom of peaceful assembly and of association (Clement Nyaletsossi Voule), the Special Rapporteur on the situation of human rights defenders (Mary Lawlor), and the Special Rapporteur on the right to privacy (Ana Brian Nougrères).

and has the potential to create a worrisome scenario in which the electronic messages of journalists, human rights defenders and other critical (marginalised) voices could be monitored. Even though the Law stipulates that monitoring would only be permissible without a judicial order in cases of "'security requirement or urgency' or when the content in question is counter to 'public morality'" (ibid.), the respective terms are – in opposition to the above-mentioned principles – imprecise and not concretised in the Law and thus there is the possibility that they will be broadly applied. Furthermore, Article 7 enables NISSA to block access to websites and content – seemingly without judicial oversight – if it provokes "racial or regional slurs and extremist religious or denominational ideologies that undermine the security and stability of the society" (United Nations Human Rights Council 2022: 10). As we highlighted in the previous chapter (4.1.) on the expansive scope of examples of national cybercrime laws, this lack of precision and (procedural/judicial) safeguards could lead to widespread violations of the right to privacy and the right to freedom of opinion and expression. Given Libya's limited progress on gender equality, the illegality of homosexuality and the prohibition of abortions in the country's Penal Code (UN Women n.d.; UNFPA et al. 2019), it is likely that content on sexual and reproductive health and rights or anything related to gender diversity would fall under this provision. Additionally, the Law codifies that the use, production and distribution of encryption technology must be granted by NISSA, which further puts the work and security of government critics, human rights defenders, and other historically or politically marginalised groups in danger (ibid.).

In Tunisia, the Decree-Law 54 not only opens the door to the criminalisation of free speech (see Chapter 4.1.) but also contains insufficient legal guarantees to protect the right to privacy. This is one of the key findings of the international digital rights organisation Access Now's 2023 report on Decree-Law 54[24], suitably titled "Freedom of expression at risk in Tunisia: a legal framework that favors silence". According to both Access Now's and Amnesty International's analyses, especially Articles 6, 9, 10, and 35 of Decree-Law 54 grant state authorities overly broad surveillance powers, permitting them to collect personal data on grounds such as it "might help to reveal the truth" and to share such information with foreign governments (Zaghdoudi 2023; Amnesty International 2022). The Law also obliges telecommunications providers "to store customers' personal data en masse so that authorities may access them [for at least two years]" (Amnesty International, 2022: 3). According to the OHCHR, such laws "exceed the limits of what can be considered necessary and proportionate" (United Nations High Commissioner for Human Rights 2018: 6; cited in ibid.).

The 2018 Egyptian Cybercrime Law raises similar alarming issues and authorises mass surveillance. Internet service providers are forced to "store customer usage data for 180 days, including data that enables user identification, data regarding content of the information system, and data related to the equipment used" (Access Now 2018) and national security authorities are allowed to access and review such data (ibid.). While the Law allows for the violation of both the right to privacy and the freedom of expression and causes self-censorship (as in the above-mentioned cases), it also has wider consequences for the online space as platforms "start to operate with a constant fear of criminal accountability, opting to remove content rather than risk the possibility of prosecution" (Ben-Hassine & Samaro 2019).

[24] The full report can be accessed here: FoE-Report-English-Final.pdf.



4.2. THE NEED TO PROTECT DIGITAL (CIVIC AND PUBLIC) SPACES AND PRIVACY: ABOUT STATE SURVEILLANCE ON THE BASIS OF NATIONAL CYBERCRIME LEGISLATION AND ITS SILENCING EFFECTS

Oppressive government control of information and communication online includes a chilling effect, i.e. especially politically or historically marginalised individuals and groups (journalists, human rights defenders, whistle-blowers, dissidents, etc.) are likely to begin to use the internet less or in a self-censoring manner, which will have considerable personal as well as societal impacts. Individuals, groups, and organisations will experience more limited access to information, have a reduced ability to mobilise for social and/or political change, and participate less in political discourse online and/or at least change the way they participate (e.g. share less criticism of the government). This particularly impacts the work of journalists and human rights defenders, especially in contexts of authoritarianism and democratic backsliding, where the freedom of speech is already limited in offline spaces. Along with such developments on an individual level, civic and public spaces online where the exchange of political opinions and ideas takes place – will continue to shrink, further aggravating trends of autocratisation and democratic backsliding.

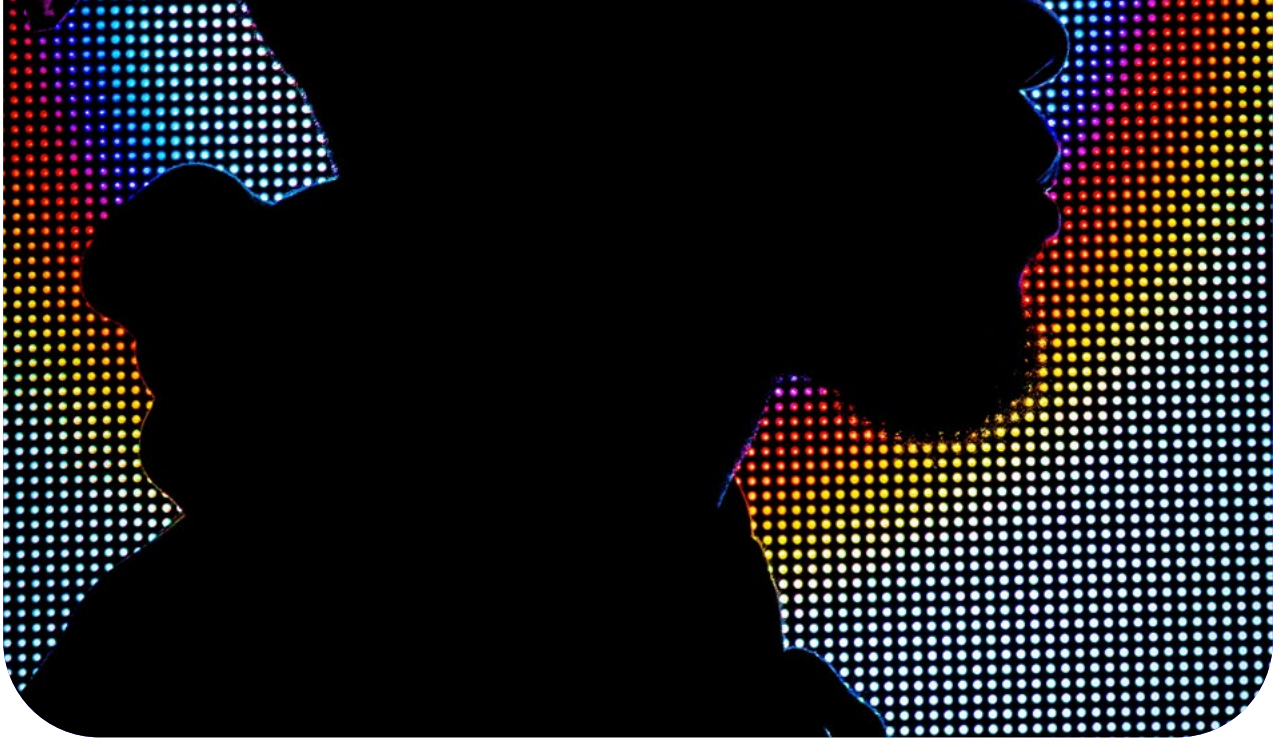
4.3.ACCESS TO JUSTICE, RIGHT TO DUE PROCESS AND RIGHT TO EFFECTIVE REMEDY

Victims and survivors of cybercrime as well as those prosecuted under oppressive cybercrime, legislation in a discriminatory (gendered) and unlawful manner, often face additional harm when seeking access to justice when being detained and/or sentenced to prison. Both (gendered) systemic biases and, in an at least partially connected way, authoritarian agendas represented in the legal systems of patriarchal societies make it more difficult for women, LGBTQIA+ people and other marginalised groups to seek redress and/or to hold states accountable in cases of overreach (see Chapter 2)[25]. Such compounding harm includes cases in which the harmful experiences of those affected by cybercrime were ignored, downplayed or discredited, as well aswhere they were unlawfully and/or unfairly treated or where they experienced intended or unintended re-victimisation.

When gendered harm compounds

The above-mentioned Ugandan feminist activist Stella Nyanzi, for example, experienced gendered harm within the justice system in several instances. In addition to a violation of her freedom of expression (as mentioned above, p. 25), the United Nations Working Group on Arbitrary Detention (WGAD) rendered an opinion[26] that found that Nyanzi's "arrest and detention amounted to a violation of her rights to [...] a fair trial, the presumption of innocence, liberty and security of person, and freedom from torture or to cruel, inhuman or degrading treatment" (Columbia University n.d.). After being forcibly arrested by members of the police dressed in civilian clothes, Nyanzi was detained, physically assaulted and, for 18 hours, denied access to a lawyer as well as to period products (ibid.). In an interview with The Guardian, Nyanzi shared further instances of purposeful, clearly gendered harm she experienced in prison, "[they were] telling us to undress before other [prisoners]" (Mwesigwa 2017).

[25] As mentioned above in footnote 14, this briefing acknowledges that (gendered) systemic biases can be found in both democratic and authoritarian countries, including in their respective legal systems and/or criminal codes.
[26] When Nyanzi was detained in a maximum-security facility, the WGAD sent a communication to the Ugandan government in connection with her detention, to which Uganda never responded (Global Freedom of Expression Columbia University, n.d.).



When cybercrime law becomes part of a systemic package deal to suppress critical voices

In Jordan, Amnesty International[27] has examined how authorities are using an additional layer of repression in connection with (threatened) charges related to pro-Palestinian solidarity under Law No. 17 (see p. X). The two cases presented below highlight how cybercrime legislation can be misused as part of a package of repressive measures to intimidate and punish critical voices, making it even more difficult for them to obtain justice and remedy. The Jordanian so-called Crime Prevention Law allows for administrative detention without charge or trial, and with limited judicial review, thus undermining fair-trial safeguards that are normally necessary in criminal proceedings under the Jordanian Law of Criminal Procedure (Amnesty International 2024b). The activist Majd al-Farraj was charged under the Jordanian Cybercrime Law No. 17 in December 2023, after he had posted pro-Palestinian content on social media. While he was acquitted by a criminal court later, he was re-arrested during a protest and held in administrative detention for over a month. A similar strategy was used by Jordanian authorities when they arrested activist Samer al-Qassem in April 2024 after he posted a TikTok video about Palestinian refugees. As Amnesty International reports, he was first released on bail about three weeks later, but the Amman governor requested his administrative detention for another month (Amnesty International 2024b). On 30 June 2024, al-Qassem was charged under Law No. 17 for "using social media platforms to provoke sedition and threaten societal peace", including a three-month prison sentence and a fine of 5,000 JOD (around 7,000 USD) (ibid.). Human Rights Watch has documented similar cases and learnt from Jordanian lawyers and activists that "in many cases, even after the public prosecutor or a judge ordered a detainee released, Interior Ministry authorities immediately re-apprehended or kept people in custody using abusive administrative detention procedures, coercing detainees to sign pledges not to protest or incite to protest under threat of a 50,000 Jordanian dinars fine (about US$70,000)" (Human Rights Watch 2024b).

[27] This section is based on Amnesty International's report from 13 August, 2024, available here: Jordan's new Cybercrimes Law stifling freedom of expression one year on.

When justice is accessible, support for victims and survivors of cybercrime is still tenuous

Most countries, including those where the justice system can be accessed through formal procedures and victims and survivors of cybercrime can enjoy their right to due process and effective remedy, still fail to create national support mechanisms that truly centre and account for the needs and experiences of those affected by cybercrime. Often, survivors are re-traumatised or re-victimised by actors within the justice system or by society as a whole (Leukfeldt, Notté & Malsch 2019; Robalo & Abdul Rahim 2023).

A 2021 study on the psychological impacts of victimisation of those who were hacked not only highlights negative direct effects (e.g., anxiety, depressive symptoms, a sense of violation of personal security, privacy, and control) but also indirect long-term impacts on victims' mental health (Palassis, Speelman & Pooley 2021). While some hacking victims encountered a lack of support from service providers, others experienced secondary victimisation through victim-blaming and generally felt help- and powerless (ibid.). Similar issues and related criticism of law enforcement and other responsible national authorities have been voiced by victims and survivors of other forms of cybercrime, too. In the case of sextortion – a gender-based cybercrime that has rapidly increased in numbers and particularly affects teenagers globally, even leading to suicides (Gavrilovic Nilsson et al. 2019), e.g. in the United States and the United Kingdom (McCubbin 2024; Smith & Crawford 2024; Tidy 2024) – police are often not adequately trained to treat those affected in a gender-sensitive way thus making victims "feel like a criminal" (McCubbin 2024). Apart from (gender-disaggregated) statistics and legal support for victims of (gendered) cybercrime, there is also a lack of national psychological/emotional support services (such as support groups) and awareness raising efforts from the state. The latter is crucial for the reduction of stigma, encouraging survivors to report, e.g., sextortion cases to the police and reducing re-victimisation of cybercrime victims by society.

Against this backdrop, victims and survivors of cybercrime have sought support from global or national civil society organisations. To provide a few examples, the UK charity Victim Support publicly provides information on crimes, the criminal justice system, and free, independent, and confidential advice for victims. The digital rights organisation Access Now established, amongst other measures, the "Digital Security Helpline" operating 24/7 in nine languages, and the Pakistani Digital Rights Foundation manages the "Cyber Harassment Helpline" which provides legal advice, psychological counselling and a referral system to victims of online harassment. SMEX, a Lebanese digital rights NGO, operates the Digital Safety Helpdesk, which supports and guides activists, journalists, human rights defenders and other marginalised groups in West Asia and North Africa through cyber-related incidents.

4.4. CASCADING AND COMPOUNDING EFFECTS

The case studies presented above have shown how overly broad cybercrime legislation and patriarchal, repressive justice systems impact the freedom of speech, the right to privacy, the right to access justice, and the security of vulnerable and marginalised groups online and offline more broadly. An intersectional feminist perspective, however, reveals further cascading and compounding impacts of cybercrime and/or cybercrime legislation, significantly increasing the total harm experienced by those who are already targeted under oppressive cybercrime laws.

When gendered harm caused by cybercrime leads to more gendered harm caused by cybercrime legislation

In terms of both compounding and cascading effects, the case of Yamen, a 25-year-old gay Jordanian man and the case of Aya, a 17-year-old influencer, illustrate the catastrophic situation in which an already marginalised individual who is affected by a gendered cybercrime faces additional harm due to state overreach discriminating against gender and sexual minorities.

Yamen became a victim of sextortion after a man he met on a dating app threatened to post a video of them having cybersex online. Consequently, Yamen filed a complaint to a special cybercrime unit in Jordan (Jain 2024). Not only was his case ignored, but Yamen – who had tried to protect himself from gender-based online violence – himself was charged under Article 9 of the Jordanian Cybercrime Law No. 17 for "soliciting prostitution online" (ibid.). During his judicial process, Yamen also faced gender-based discrimination by state agents when he was "feminised" as "the one who wanted to seduce the guy", as he states in an interview with Human Rights Watch (Human Rights Watch 2023c). He was imprisoned for one month and had to pay a fine (ibid.).

In 2022, Aya, who is known as "Menna Abdelaziz" on social media, was affected by similar compounding harm after facing sextortion. As Human Rights Watch reports, the 17-year-old was beaten up by a group of men and women, and raped by some of the men, who also filmed the acts and then blackmailed her with the footage. After Aya posted a video to share her experiences online, she was arrested by the Egyptian authorities. Two days later, "the Office of the Prosecutor General

[23] The commentary was written by the Special Rapporteurs on the promotion and protection of the right to freedom of opinion and expression (Irene Khan), the Special Rapporteur on the rights to freedom of peaceful assembly and of association (Clement Nyaletsossi Voule), the Special Rapporteur on the situation of human rights defenders (Mary Lawlor), and the Special Rapporteur on the right to privacy (Ana Brian Nougrères).

issued a statement saying prosecutors ordered her detained pending investigation as a victim of sexual assault but also as a suspect in morality-related offenses for her videos generally" (Human Rights Watch 2020). Even though the men and women responsible for the assault and rape were prosecuted in a criminal trial, Aya was sent to a women's shelter, the investigations on grounds of "morality" under the 2018 Cybercrime Law No. 175 continued. This created serious and multiple compounding harm. The additional violation of Aya's freedom of expression and the connected (re-)victimisation she faced under Law No. 175 significantly adds to the psychological and physical harm she experienced as a victim and survivor of sexual violence and sextortion (see p. X). Human Rights Watch has called for the Egyptian authorities to immediately release Aya from detention "while ensuring her safety and that she receives appropriate care" (Human Rights Watch 2020) with reference to international law that "prohibits the detention of children except as a last resort and for the shortest appropriate period of time" (ibid.).

When state-mandated restrictions of the freedom of expression lead private actors to actively restrict civic spaces, too

In terms of cascading effects, consider the case of the Jordanian Cybercrime Law No. 17. Shortly after the Law was approved, Amnesty International was informed by two independent news platforms that they had removed their comment section due to Article 33 of the Law, allowing "the prosecutor or court [to] order any website, social media platform, or person responsible for a public account to remove or block content deemed to have violated the law, to temporarily ban the user or publisher, and to hand over relevant information, including users' personal data" (Amnesty International 2023). While Law No. 17 has already seriously restricted social media users' freedom of expression online, especially in terms of pro-Palestinian protest and solidarity as highlighted above, these same users face further constraints due to media outlets restricting the options to voice one's opinion on news content out of fear of being prosecuted. Such developments lead to the continuous shrinking of civic online spaces (see also Hassan & Hellyer 2024) "at a time when people in Jordan are already deprived of spaces and forums to express their opinions" (Amnesty International 2023), which could be seen as a compounding effect.

This chapter has highlighted how national cybercrime laws are used as a tool for state overreach, disproportionately targeting women, LGBTQIA+ people and activists, journalists, human rights defenders, and other critical voices and marginalised groups. Instead of protecting citizens and safeguarding fundamental freedoms and human rights, many governments, particularly in authoritarian contexts, exploit vague and overly broad cybercrime laws to suppress dissent, criminalise free speech online, and enable targeted and/or mass state surveillance. Along with marginalised groups' limited access to justice, this often leads to self-censorship and further shrinks digital civic spaces. These laws frequently invoke concepts like "public morals" or "national security" to justify restrictions on (digital) human rights, reproducing and reinforcing (offline) patriarchal and autocratic discriminatory power structures in and through online space. This chapter underscores the urgent need for cybercrime laws that adhere to human rights principles and ensure, amongst other rights, privacy, non-discrimination and freedom of expression.

[24] The full report can be accessed here: FoE-Report-English-Final.pdf.

5. THE UN CYBERCRIME CONVENTION

Building on the lessons and insights from the national contexts explored above, this chapter analyses the UN Cybercrime Convention from an intersectional feminist perspective. We highlight both the opportunities that the treaty can create as well as its risks, pitfalls and potential for misuse, in order to prevent negative impacts similar to those demonstrated in Chapter 4.

INFOBOX 3

THE UN CONVENTION AGAINST CYBERCRIME

In 2019, following an initiative by the Russian Federation, the UN General Assembly voted to establish an open-ended ad hoc intergovernmental committee in the UN General Assembly Resolution 74/247, under the auspices of the UN Third Committee, with a mandate to draft a convention combating cybercrime. After an organisational session in May 2021, the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (short: AHC) launched its substantive work in February 2022. It delivered a draft convention at the reconvened concluding session in August 2024. The document was approved by the General Assembly in December that year.[28] The multistakeholder community, comprising representatives from civil society, the private sector, academia, and the technical community, provided input during the negotiations according to the modalities for multistakeholder participation (AHC 2021). Stakeholder involvement in the AHC process was widely recognised for its inclusive approach, however, the multistakeholder community concluded that the final document did not adequately address the raised concerns, making the instrument prone to potential future misuse.[29]

[28] For a more detailed overview of the process leading up to the adoption of the Cybercrime Convention, see the AHC's official website: Ad Hoc Committee - Home.

[29] Amongst those actors were various human rights and media freedom organisations (see, e.g., their Joint Letter to the EU which CFFP also signed; Access Now 2024; Human Rights Watch 2024d), the Office of the UN High Commissioner of Human Rights (2024), security researchers (Gullo 2024) and the Advisory Network of the Freedom Online Coalition (2024), as well as the tech industry (Cybersecurity Tech Accord 2024a; Microsoft 2024) and other private sector associations (International Chamber of Commerce 2024).

5.1. UN CYBERCRIME CONVENTION AND GENDER

Despite early resistance from some states, which argued against singling out gender in the Convention, gender featured prominently in the AHC discussions. These debates highlighted the complex intersection of gender and cybercrime (Hakmeh 2025). Several member states noted their support for provisions acknowledging the specific risks that cybercrime poses to women and girls in the form of TFGBV, as well as to boys, especially regarding child sexual abuse material online. The delegations proposed incorporating gender equality, as a component of human rights, directly into the general and mainstreaming gender across the Convention (Chatham House 2022). In the preamble, the final text affirms the importance of mainstreaming a gender perspective to prevent and combat cybercrime. The emphasis on the importance of addressing online gender-based violence is tangible in Article 53 (h) on preventive measures, which proposes "developing strategies and policies, in accordance with domestic law, to prevent and eradicate gender-based violence that occurs through the use of an information and communications technology system, as well as taking into consideration the special circumstances and needs of persons in vulnerable situations in developing preventive measures". Although this reflects a recognition of the differentiated impacts of cybercrime on individuals based on their gender, the treaty falls short of incorporating broader gender-sensitive and gender-responsive approaches. Stronger and more prescriptive language that explicitly requires states to actively safeguard non-discrimination rights, while affirming a commitment to gender equality, would be welcome in the UN framework.

5.2. EXPANSIVE SCOPE MAY TURN THE CONVENTION INTO A GENERAL DATA ACCESS TREATY

The previous chapter showed how broad provisions and vague definitions can lead to arbitrary or discretionary enforcement, often targeting women, marginalised groups and individuals in vulnerable situations. Despite the substantial evidence and significant risks involved, the Convention applies a broad scope throughout the text, notably in chapters on international cooperation and procedural measures. Combined with only minimal safeguards, this instrument bears the potential to produce unintended and adverse consequences. For example, under Article 35 (c) on general principles of international cooperation, states agreed to cooperate beyond criminal offences established in accordance with the Convention and extend the cooperation to "collecting, obtaining, preserving, and sharing of evidence in electronic form of any serious crime". As specified in Article 2 (h) on terminology, serious crime is defined as "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty". Although the inspiration for this definition is derived from the UN Convention Against Transnational Organised Crime (UNTOC), the enforcement related to cybercrime offences may result in the unprecedented expansion of the new instrument's application (Tennant & Oliveira 2024). Considering how much of modern life takes place online, there will be electronic evidence of almost every serious crime under any domestic legislation.

The provision most suited to the prevention of potential misuse is included in Article 6, stating that "nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law". This general provision applies to the entire text and should guide the application of the Convention and its translation into national frameworks (Walker & Oliveira 2024). The rest of the human rights safeguards are bound to specific chapters. Concerning international cooperation, Article 40 (22) on general principles and procedures relating to mutual legal assistance further notes that "nothing in this Convention shall be interpreted as imposing an obligation to afford mutual legal assistance if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person's sex, race, language, religion, nationality, ethnic origin or political opinions…". However, this may not provide effective safeguards for the rights and freedoms of individuals, especially those that may be already overly targeted and marginalised. If the offence is punishable in both countries which decide to cooperate by exchanging electronic evidence, the instrument can open doors to potential misuse. In this way, even provisions that do not explicitly relate to gender can have significant gender-specific effects depending on how these articles are interpreted and enacted.

For illustration, the Convention could oblige law enforcement agencies to cooperate in prosecuting the LGBTQIA+ community and its defenders. In Russia, association with the "international LGBT movement" can lead to extremism charges (Human Rights Watch 2024c). Acts such as displaying the rainbow flag, which can be considered an "extremist group symbol", can lead to criminal convictions. A first conviction carries a penalty of up to fifteen days in detention, but a repeat offence carries a penalty of up to four years. A repeat offence would qualify as a "serious crime" under the Convention and be eligible for assistance from law enforcement in other jurisdictions (Rodriguez 2024). Displaying any association with the LGBTQIA+ community can, therefore, result in the collection of electronic evidence relevant to the investigation, including traffic, subscriber and even content data, and in the sharing of evidence between countries. Similar considerations apply to accessing sexual and reproductive health if certain actions are criminalised by domestic law. Some twenty-two countries have total bans on abortion, while many others permit abortion only under specific conditions (Council on Foreign Relations 2024). The treaty could potentially allow for the collection of location data to track visits to healthcare facilities, information from fertility tracking apps, or browser histories of individuals searching for sexual and reproductive health services in their area (Chatham House 2022; Gollan 2023).

Considering the multiple, complex, and far-reaching risks, the safeguards related to data protection and privacy in the treaty are inadequate. The preamble includes a paragraph stipulating the right to protection against arbitrary or unlawful interference with one's privacy, and the importance of protecting personal data. This reference recognises the risk that governments might arbitrarily interfere in people's privacy with the measures enabled by this instrument but does not carry the weight necessary to prevent such conduct. In the implementation, specific and strengthened privacy protections should be afforded for protected forms of communication, including medical, legal, religious or public interest. Such distinctions are necessary to ensure the rights and well-being of women and people of diverse gender identities, expressions and sexual orientations both broadly and in jurisdictions where access to abortion and/or the expression of LGBTQIA+ identities are currently not legally permitted (Chatham House 2022).

5.3. PROBLEMATIC MUTUAL LEGAL ASSISTANCE AND DATA COLLECTION

Under the banner of fighting cybercrime, the UN Convention will result in more individuals' private information being shared with more governments around the world. While the sharing of electronic evidence between law enforcement agencies is necessary to combat transnational cybercriminal activities, the text weakens the ability of democratic countries to refuse problematic requests submitted by authoritarian states. The requirements for international cooperation can weaken a country's ability to dissuade other states from assisting in improper, suppressive investigations launched by oppressive governments (Adams & Podair 2024). Article 40 requires states to provide the "widest measure" of mutual legal assistance in law enforcement investigations under the treaty. Because general principles and procedures relating to mutual legal assistance are broad and decoupled from strong safeguards, the provisions will allow authorities to proceed without meaningful transparency or accountability mechanisms. States may decline to render assistance on the grounds of the absence of dual criminality. However, they may also decide to provide assistance, irrespective of whether the conduct would constitute an offence under their domestic law. The provision on legal assistance fails to note any restriction on whether the data in question are even located in the territory of the assisting state. Furthermore, Article 22 includes a provision that could authorise states to exercise jurisdiction over extraterritorial conduct that harms their nationals, also known as passive personality jurisdiction. This provision risks legitimising cases where states apply their domestic criminal codes extraterritorially and then leverage their power to target foreigners abroad (Scher-Zagier 2024).

Many individuals whose information is transferred will be persons of interest who are never charged with an offence. The Convention does not include a safeguard that would require responsible authorities to inform these individuals if governments have requested and gained access to their private information, rendering affected persons unable to protect themselves and defend their rights (Cybersecurity Tech Accord 2024b). Extensive procedural powers without the necessary transparency and oversight measures carry a significant risk of state overreach. In this context, the Convention's provisions, which give states the permission to "collect or record" relevant data for a conviction and "compel" service providers to

hand over incriminating information or documents, are problematic. The text facilitates secret access to secured systems, extraterritorial exfiltration of data and secret real-time data collection without sufficient and robust conditions and safeguards to ensure that states adhere to what is necessary and proportionate for legitimate measures addressing cybercrime. The treaty scarcely mentions the principles of necessity and proportionality and defers to domestic law for human rights safeguards instead of international human rights frameworks. If countries have not incorporated their international obligations into domestic laws or violate human rights in practice, the Convention does not oblige authorities to consider international standards when implementing its provisions. In this context, the fact that countries with poor human rights records, including Belarus, China, Iran, Nicaragua, Cuba and Russia, have been strong proponents of the Convention does not help to establish trust in the instrument. In an unsuccessful last-minute bid, Iran called for votes to have references that safeguard human rights removed (Walker & Oliveira 2024).

The Convention incentivises the procurement of surveillance capabilities necessary for carrying out cybercrime-related investigations. While the use of dual-use technology and surveillance software can be legitimate for certain investigative purposes, it also inadvertently facilitates state overreach in the form of both targeted and mass surveillance and advanced detection and censorship capabilities. Article 28 on the search and seizure of stored electronic data requires signatories to empower the competent authorities to obtain surveillance capabilities over stored electronic data in their territory. Articles 29 and Article 30 oblige states to acquire the capability to carry out intrusive practices such as the real-time interception of traffic data and content data. These provisions do not include an obligation to conduct human-rights impact assessments of these activities nor do they prohibit states from turning to commercially available cyber intrusion capabilities and provide additional fodder for the cyber mercenary market.

[23] The commentary was written by the Special Rapporteurs on the promotion and protection of the right to freedom of opinion and expression (Irene Khan), the Special Rapporteur on the rights to freedom of peaceful assembly and of association (Clement Nyaletsossi Voule), the Special Rapporteur on the situation of human rights defenders (Mary Lawlor), and the Special Rapporteur on the right to privacy (Ana Brian Nougrères).

5.4. EXTREMISM- AND TERRORISM-RELATED OFFENCES DO NOT BELONG IN A LEGALLY BINDING CYBERCRIME TREATY

The negotiations involved significant debate over the inclusion of content-related offences, such as extremism and terrorism-related offences, and the dissemination of false information.[30] These references raised an alarm, as there are no universally agreed-upon definitions of extremism and terrorism under international law. States have often leveraged these highly subjective terms to justify repressive measures that disproportionately restrict the rights to free expression, assembly, opinion and belief. As evidenced in the case studies above (see Chapter 4), content-related offences considered under the cybercrime law can have far-reaching damaging effects on individuals, especially women persecuted by patriarchal and autocratic regimes, marginalised groups and targeted individuals such as human rights defenders, journalists and political dissidents. As highlighted by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, "in many parts of the world, any form of expression that articulates a view contrary to the official position of the State, addresses human rights violations and comments on ways to do things better, in accordance with human rights obligation, constitutes a form of terrorist activity or violent extremism or a broad 'threat to national security', which often encompasses both terrorism and extremism". Some countries use these provisions to suppress civil society and silence defenders of LGBTQIA+ rights (United Nations Human Rights Council 2019b). Absent a clear, narrow definition of terrorism and extremism that comports with international human rights standards, such references in the Convention would risk perpetuating human rights violations by expanding the application of already overbroad counterterrorism laws to cybercrime.

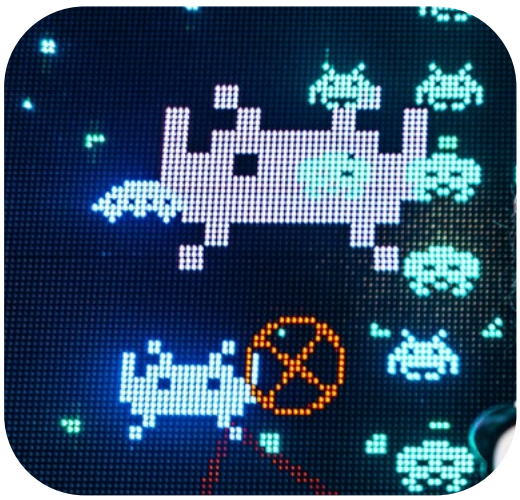
There is an alarming rise in the use and misuse of cybercrime instruments and legislation by some states to target activists, journalists, whistleblowers, members of the opposition and minorities by citing national security concerns, maintaining social order, and fighting extremism, terrorism or fake news. Any such reference in an international framework such as the Convention would allow governments to pass domestic laws that criminalise free speech, if it is committed through online means, and point to the UN or other international instruments to justify the enforcement of repressive measures. The criminalisation chapter in the final document, which lists specific crimes that the treaty aims to address, is focused primarily on cyber-dependent provisions. However, the Convention allows for protocols (Articles 61 and 62) and does not designate specific issues that can be covered in them. Therefore, additional protocols may be used in the future to try to expand the scope to speech offences, as suggested by Russia during negotiations (Walker & Oliveira 2024).

[30] The consolidated negotiating document (status as of 21 January 2023) can be accessed here: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf .

5.5. CSAM AND NCSII

Content-based offences included in the criminalisation chapter cover offences related to online child sexual abuse or child sexual exploitation material (Article 14), solicitation or grooming for the purpose of committing a sexual offence against a child (Article 15) and non-consensual dissemination of intimate images (Article 16). Child sexual abuse or child sexual exploitation material (CSAM) is understood as content depicting or otherwise related to the sexual abuse or exploitation of a child or young person, including images, videos or live-streamed content depicting real children being sexually abused. The Convention addresses CSAM in the form of producing, offering, selling, distributing, transmitting, broadcasting, soliciting, procuring, accessing, possessing and financing such content. The fight against CSAM is paramount, especially given its long-term devastating effects on the victims and the prevalence of this crime, but the provisions risk wider criminalisation. The scope of child sexual abuse could subject legitimate online activities to criminal prosecution and result in serious human rights violations, including the prosecution of children. Specifically, these provisions could lead to persons under 18 years of age who take "naked or sexually suggestive selfies" being charged with criminal offences. The article includes a concluding reference that "nothing in this Convention shall affect any international obligations which are more conducive to the realisation of the rights of the child", however, this may not prevent the criminalisation of children by articles which are supposed to protect them from harm (Hollingworth 2024).

The Convention criminalises the sharing of private materials of a sexual nature, either photos or videos, of another person without their consent (Article 16). The inclusion of non-consensual dissemination of intimate images (NCIID) is a pivotal moment, offering an international framework for preventing, investigating and prosecuting image-based abuse. NCIID is part of online gender-based violence, since women and girls and people of diverse gender identities, expressions, and sexual orientations experience more vulnerabilities to this form of online harm (Chatham House 2022). Furthermore, the connected extortion schemes frequently involve international crime groups exploiting vulnerable individuals. Often referred to as "revenge porn" laws, provisions connected to NCIID exist in various forms in a significant number of countries. Still, many others do not recognise this crime, lack the necessary legal frameworks, or address NCIID inadequately. Heightened awareness of and attention to NCIID and other exploitative crimes is essential, especially when accompanied with the capacity needed to investigate and prosecute these crimes and to address them in a gender-sensitive manner. For instance, the South West Grid for Learning (SWGfL), an NGO working with the Revenge Porn Helpline and StopNCII.org, anticipates that the Convention will empower online platforms, governments and civil society to act swiftly and decisively when content is shared without consent. This recognition in an international cybercrime framework potentially paves the way for more robust partnerships to ensure that victims receive the necessary assistance, support, and redress (Wright 2024).



5.6. VICTIM SUPPORT AND WITNESS PROTECTION

Cybercrime affects individuals differently based on their gender identity and expression and other identity markers such as race (see Chapter 2). These differentiated impacts necessitate gender-sensitive witness and victim protection mechanisms adjusted to the individual's specific needs. Otherwise, the initial harm can be exacerbated by inadequate responses that intensify existing vulnerabilities and societal inequalities and hinder access to justice and remedy. In the preamble, the treaty recognises "the increasing number of victims of cybercrime, the importance of obtaining justice for those victims and the necessity to address the needs of persons in vulnerable situations in measures taken to prevent and combat the offences covered by this Convention." The provisions on assistance to and protection of victims (Article 34) further stipulate that states should "provide assistance and protection to victims of offences established in accordance with this Convention, in particular in cases of threat of retaliation or intimidation." This encompasses compensation and restitution for victims, including for their physical and psychological recovery, in cooperation with relevant international organisations, non-governmental organisations, and other elements of civil society. In applying these provisions, states should "take into account the age, gender and the particular circumstances and needs of victims, including the particular circumstances and needs of children". Unfortunately, the text makes the needed assistance and protection merely optional and defers to domestic law that may not contain effective protections. The victims are, therefore, left solely to the consideration of national agencies, many of which employ discriminatory practices. This leaves victims with no legal guarantees or rights to seek recourse and return of property.

Similar considerations apply to Article 33 on witness protection. States are requested to provide witnesses with effective protection from potential retaliation and intimidation and to establish procedures for the physical protection of such persons, but domestic legislation may not offer adequate protection, remedies and redress mechanisms, and states are not incentivised to align themselves with international standards. The fight against cybercrime must consider the significant human impact and harm it has, often targeting the most vulnerable individuals. Therefore, it is paramount that states, in the implementation of the Convention, apply best practices, such as developing partnerships between law enforcement, legal professionals, and victim support organisations to strengthen victim-centred approaches.

Next steps

According to Article 64, the Convention enters into force after the 40th member state deposits its ratification, acceptance, approval or accession to the treaty. However, there is no timeline for member states to do so. While the adoption of the agreed text in the UN General Assembly was seen as a formality, as the states had already reached a consensus on the draft resolution in the reconvened concluding session of the AHC, the ratification process may be lengthy. The states that have agreed with the Convention internally will mainly depend on parliaments and countries' domestic systems to consent to be bound by international instruments. Therefore, the treaty's implementation will depend on the legislative branches of many jurisdictions, delaying the process for the treaty to enter into force (Walker & Oliveira 2024). The implementation is expected to be inconsistent and vary significantly across countries. Despite this foreseen unequal progress, the document is set to shape cybercrime laws worldwide. Its effectiveness and whether it will do more good than harm will hinge on which states ratify the instrument and its subsequent implementation. Therefore, it is essential for civil society and human rights organisations to actively engage in providing feedback on the implementation process and conduct diligent monitoring of how the provisions are translated into national frameworks. Where the responsible agencies have histories of discrimination and repression against certain gender identities, sexualities or sexual orientations, as well as other marginalised groups, discriminatory practices are likely to manifest in domestic law and criminal procedural powers in the name of fighting cybercrime (Shires, Hassib & Swali 2024).

6. THE WAY FORWARD: RECOMMENDATIONS FOR NATIONAL GOVERNMENTS, UN INSTITUTIONS, AND NON-GOVERNMENTAL ACTORS

Taking an intersectional feminist perspective on cybercrime legislation, this policy briefing has demonstrated how national cybercrime legislation is often misused and instrumentalised by states. State overreach has differentiated, as well as potentially compounding and cascading, effects on individuals and groups, many of whom are already discriminated against and marginalised on the basis of gender and/or other (intersecting) identity markers. Under the pretext of fighting cybercrime, governments have silenced critical voices, suppressed dissent, limited human rights and LGBTQIA+ activism, and curtailed journalistic reporting and media freedoms.

Legislative overreach in the form of national cybercrime legislation can lead to shrinking civic spaces online and serve to advance authoritarian, anti-democratic and anti-feminist agendas (see Chapter 4). Such practices underline the need for human rights-centred, gender-responsive and intersectional feminist approaches to cybercrime governance. The UN cybercrime negotiations provided a window of opportunity to anchor such considerations at the international level. However, as the previous chapter highlighted while being informed by lessons learned from national contexts (Chapter 4), the adopted treaty presents multiple risks. This potential for misuse must be adequately addressed in states' decisions on when and whether to sign and ratify the instrument and in future implementation efforts and oversight mechanisms.

The following policy recommendations provide states with guidance concerning cybercrime legislation, and particularly the implementation of the UN Cybercrime Convention, regardless of their position on signature/ratification and/or preparation for the future implementation of the treaty. They are by no means exhaustive and aim to incentivise inclusive multistakeholder participation and the adoption of human-rights-respecting and intersectional feminist perspectives.

POLICY RECOMMENDATIONS

1. Actively include and engage with the multistakeholder community in discussions and consultations on the decision to sign and ratify the UN Cybercrime Convention and, if applicable, in discussions on the future implementation of the treaty.

Against the backdrop of the UN Cybercrime Convention's weaknesses and pitfalls (see Chapter 5), it is crucial that **(feminist and human rights) civil society organisations, the private sector and the expert community serve not only as watchdogs but also as guides**, ensuring the framework is implemented in a way that respects human rights and follows an intersectional feminist approach to cybercrime legislation. For this effort to be effective, states need to actively engage with the multistakeholder community and include civil society organisations in consultative processes on the final decision concerning the signing and ratification of the UN Cybercrime Convention and, if applicable, in the treaty's implementation phase.

Therefore, states should create and **institutionalise a regular multistakeholder consultation mechanism** both at their respective national levels and at the international level, i.e. at the UNODC and at the Conference of States Parties to the UN Cybercrime Convention (see Article 57, given it enters into force). Such a mechanism and related processes, as well as any other exchange with the multistakeholder community, should be **designed inclusively and be easily accessible**, i.e. be sensitive to participants' constraints and integrate financial and (if applicable) visa support for participants, especially for civil society representatives and/or activists and experts from the so-called Global South. Moreover, online participation must be made possible, and the modalities of AHC 1 should be continued in AHC 2.

2. (Re-)Consider if signing the UN Cybercrime Convention is compatible with commitments to human rights and fundamental freedoms or other (political) commitments.

In addition to the above-mentioned multistakeholder consultations, states and the European Union (EU) should make sure to **seek all available sources of information and (judicial) review procedures** to test whether the UN Cybercrime Convention is compatible with established (legal) commitments to human rights, fundamental freedoms, and other (political) commitments to feminist concepts, principles and goals, such as a Feminist Foreign Policy. In the case of the EU, an Advisory Opinion by the European Court of Justice should be requested by an EU member state, the EU Commission, the European Parliament or by the Council to clarify "as to whether an agreement [the UN Cybercrime Convention] envisaged is compatible with the Treaties" (Treaty on the Functioning of the European Union, Art. 218 (11)).

3. Commit to established human rights principles and safeguards in the implementation of the UN Cybercrime Convention and closely monitor the rights-respecting implementation of the treaty, including through adequate, effective and inclusive review mechanisms and other human-rights promoting measures, in cooperation with the multistakeholder community.

Analyses of the implementation of UNTOC and UNCAC – which can provide lessons learned for the implementation of the UN Cybercrime Convention in terms of respect for human rights – have shown that "human rights issues and languages are still a controversial theme in Vienna, where the review of implementation of both UNTOC and UNCAC takes place, and where civil society participation is par-

ticularly restrictive" (Tennant & Oliveira 2024). "If the cybercrime treaty monitoring body is also set up in Vienna, the cybercrime treaty might also face similar difficulty. Considering the human rights risks (both of criminalisation of civil society and abuse of state powers in criminal investigations), the broad and flexible approach to criminalisation is likely to cause more unintended (negative) consequences in line with what is already seen within the context of enforcing state powers in the context of UNTOC and UNCAC (for example, issues around police brutality in the context of anti-crime; witness and victims protections; and breach to due process)" (ibid.).

The **key principles on the future review mechanism** for the UN Cybercrime Convention proposed by Tennant and Oliveira (2024: 232) provide an excellent basis for states to build on. In the following, some of Tennant and Oliveira's (2024) principles were copied and expanded through the integration of an intersectional feminist perspective:

1. The mechanism of implementation needs to **centre intersectional feminist and human-rights based perspectives** which are fundamental to its success, not an afterthought.

2. The objective of any mechanism should be evaluation and impact measurement – not a pure measurement of progress of legal implementation. This includes an **intersectional gender impact assessment** (consider existing tools developed by civil society, such as Association for Progressive Communication's 2023 assessment tool) and analyses of the instrument's effect on human rights, particularly the human rights of marginalised groups, democratic processes and global Internet freedom. As part of this, the mechanism should have access to the latest (intersectional gender-disaggregated) data and evidence and actively consult and include the multistakeholder expert community in evaluation and impact assessment efforts (see Recommendation 7 below).

3. Easy and safe access to a review mechanism and an open and inclusive role for all sectors of society are crucial (see Recommendation 1) for ensuring that timely and relevant information is available, promoting accountability, engaging in potential future negotiations and monitoring implementation.

In terms of mitigating potential human rights violations through targeted/mass surveillance due to the UN Cybercrime Conventions pitfalls (see Chapter 5), states should **commit to the** "International Principles on the Application of Human Rights to Communications Surveillance" (also called the "Necessary and Proportionate Principles" or "13 Principles") that were established by an international coalition of civil society, surveillance law scholars, and privacy and technology experts and endorsed by over 600 organisations and over 270,000 individuals worldwide (see Necessary & Proportionate, n.d.). The "Necessary and Proportionate Principles" show how international human rights law applies in online space, particularly in light of modern digital surveillance. In national and international discussions, as well as with regard to the implementation of national and international legal frameworks related to surveillance and international data sharing, states should also consider the implementation guide for the "Necessary and Proportionate Principles" by Access Now (2015).[31]

[31] This recommendation was inspired by valuable discussions with experts mentioned in the imprint.

4. Promote an intersectional feminist approach to cybercrime legislation in (future) national and international norm-setting processes and discussion fora, particularly at the Conference of States Parties to the UN Cybercrime Convention (given it enters into force).

In international discussions and negotiations, particularly at the Conference of States Parties to the UN Cybercrime Convention (see Article 57), states should **highlight the differentiated impact of cybercrime on women, LGBTQAI+ people and other marginalised groups** and thus the **importance of centring their needs and lived experiences** (in additional international and their respective national legislation). Moreover, states should **point out the risks that these individuals and groups might/will face due to the weaknesses of the UN Cybercrime Convention** (see Chapter 5).
In all norm-setting efforts, states should draw from existing knowledge and resources, such as the 2023 Inclusive Cyber Norms Toolkit by Global Partners Digital.

5. When implementing the UN Cybercrime Convention at a national level and designing/adapting national cybercrime legislation (accordingly), gender-mainstream cybercrime legislation and regularly carry out impact assessments according to intersectional feminist principles and in cooperation with (feminist) civil society and the multistakeholder community.

States should mainstream gender into all cyber and anti-cybercrime related policies, legal frameworks, and practices, including a commitment to gender equality. Respective agencies should **initiate a process that critically analyses cyber- and anti-cybercrime-related policies and laws from an intersectional perspective** and include a cyber dimension in frameworks relevant to gender and gender equality (such as the Women, Peace, and Security National Action Plan, e.g.).

As shown in the previous chapters, anti-cybercrime policy and legislation can exacerbate or introduce new harms based on gender and/or other (intersecting) identity markers. **States should draw on existing knowledge and resources within the multistakeholder community**, such as the Association for Progressive Communications' (APC) A framework for developing gender-responsive cybersecurity policy: Assessment Tool, which help policy makers and implementers incorporate feminist methodologies, principles, and gender analyses and impact assessments, while promoting gender equality and preventing cyber policies from unintentionally reinforcing gender disparities.

Participatory and inclusive approaches help states to fill potential gaps within the intersectional gender analysis and impact assessment and to understand local and contextual gender dimensions and other forms of discrimination based on further (intersecting) identity markers. This includes **engaging with LGBTQIA+, women's rights and human rights groups, research institutions, and grassroots organisations with established networks and proximity to victims and survivors to encourage proportional and adequate representation of women and other marginalised groups and intersectional (gender) perspectives throughout processes of policymaking, reviewing/adapting existing laws and policies, and implementation**. Multiple stakeholders should be formally involved so they can advise and provide evidence and insight (Pavlova 2024): states should institutionalise ongoing partnerships with academia and feminist civil society, i.e. by establishing permanent (financially compensated, easily accessible) consultation mecha-

nisms (see Recommendation 1).

6. Promote and financially support capacity building, access to justice and gender-sensitive, victim-centred support for victims and survivors of cybercrime and state overreach.

Capacity building is a necessary component of an effective implementation. However, "a cautious approach is needed with regard to international capacity-building that includes non-democratic recipient countries", as unaccountable and/or repressive systems could be unintentionally supported (Hansel and Silomon 2023).

In this context, restrictions on technology transfers as part of technical assistance between countries merit careful consideration. Building up the capacity of state agencies to effectively fight cybercrime is vital for an effective implementation of the agreed-upon provisions. However, it poses risks that can eventuate into both intended and unintended harms and can have wide-ranging consequences that affect local communities (Chatham House n.d.). This is particularly the case when capacity building activities include the transfer of dual-use tools. Surveillance technologies are prone to misuse, posing substantial risks to human rights and fundamental freedoms (see Chapter 4). **Technical assistance and capacity-building ought to be subject to a human-rights and (gender-sensitive) impact assessment** that informs and guides all such activities, their scope, consequences, and the exchanged and employed tools before such activities are undertaken. These activities should also adhere to international human rights law and be subject to independent oversight.
Also, states need to **ensure that individuals and/or communities affected by cybercrime or the misuse of cybercrime legislation are not being re-victimised**: states thus need to find a balance between marginalised individuals' and groups' agency and their victimisation. The criminal justice system thus needs substantial capacity to gather evidence of and investigate the impacts of data weaponisation on the basis of gender and further (intersecting) identity markers. **Specialised training for law enforcement, prosecutors and judges** is essential for the effective handling of cybercrime cases, ensuring that they have the technical capacity and expertise to secure and verify evidence, conduct thorough investigations, and prosecute offenders in a manner that upholds justice and protects victims and survivors of cybercrimes. States should increase the capacity of the institutions and agencies responsible for countering and responding to cybercrime and further embed intersectional gender considerations (and related cascading and compounding effects) in their mandates, processes and practices. (Pavlova, 2024)

Victim assistance services should be systematically funded, and states should **increase their capacity to provide gender-sensitive and -responsive assistance that prioritises a victim-centred approach** to redress and reparations. States should create specialised Cyber Victim Support Units (CVSU) within law enforcement agencies that focus on supporting victims and survivors of cybercrime, with a particular emphasis on crimes that have a gendered component such as cyberstalking, harassment and doxing. The purpose of these units would not only be to provide a unique understanding of and support for survivors of gendered cybercrimes and cybercrimes on the basis of other (intersecting) identity markers but to raise awareness of the fact that women, LGBTQIA+ people and other marginalised groups are at a higher risk (Wong 2024).

As criminal systems and law enforcement are not gender-neutral, groups marginalised on the ba-

sis of sexuality and gender often face significant barriers to seeking help in their countries, as the examples in Chapter 4.3. have highlighted. In cases where the state is the attacker, especially in authoritarian contexts, victims and survivors of cybercrime have basically no path to obtain justice. Support for victims of gendered cyberattacks and other forms of technology-facilitated gender-based violence is currently fragmented, relying on a patchwork of civil society organisations and social justice groups. These organisations remain underfunded and thus cannot provide the comprehensive assistance essential for addressing the complex needs of victims and survivors of cybercrime or state overreach. This includes access to legal counsel, psychological support and effective remedies that prevent revictimisation (Pavlova 2024). Therefore, **victim and survivor support mechanisms established and maintained by civil society should be supported by states with financial aid as well as awareness-raising**.

For example, through the Revenge Porn Helpline, South West Grid for Learning UK (SWGfL) provides support to victims and survivors of sextortion cases which frequently involve international crime groups exploiting vulnerable individuals. With an over 90% removal rate, the helpline has successfully removed over 200,000 individual non-consensual intimate images from the Internet since it was established in 2015. Their recent data shows a 54% increase in sextortion reports over the past year, with victims also reporting high levels of anxiety and fear about their images being shared. Effective coalition building is vital for tackling cybercrime and supporting victims. In collaboration with international NGOs and technology platforms, StopNCII.org offers device-side hashing technology, allowing victims to protect their content before it spreads. By creating hash values and communicating with platforms, this tool provides real-time blocking without storing or sharing victims' data. The Argentinian project Acoso Online provides essential support and legal information in cases of NCSII and other forms of TFGBV. In all anti-cybercrime capacity building efforts, states should **draw from existing knowledge and resources**, such as Chatham House's Toolkit "Integrating gender in cybercrime capacity-building".

7. Support independent interdisciplinary academic research, especially feminist scholars, and (feminist) civil society's work on cybercrime and cybercrime legislation.

Against the backdrop of the development of new technologies and the latter's impact on the nature, intensity, and effects of cybercrime, states should ensure that they **collect gender-disaggregated data and data on cybercrime on the basis of other (intersecting) identity markers** (such as disability, class, ethnicity, race, etc.). A nuanced database is key to understanding the fast-changing cybercrime environment including its sources and perpetrators, victims and survivors, and the forms/intensity/cascading and compounding nature of harm, and to establishing well-informed policies (see also Pavlova, 2024). State agencies or other implementers tasked with the collection of such data, especially if they are in contact with victims and survivors of cybercrime, need to be trained in terms of gender- and trauma-sensitive communication in order to **avoid re-traumatisation or other harmful impacts** on those interviewed about their experiences.

States should further **support existing civil society initiatives and their efforts in collecting qualitative and quantitative evidence of cybercrimes committed on the basis of gender and other (intersecting) factors of identity** and in exploring their impact on marginalised groups. Consider, for example, the "Words Matter" pro-

ject by Democracy Reporting International (DRI) in cooperation with various local partners in the MENA region. Together with DRI and the TA-MAM Coalition, the Jordan Open-Source Association established the open-source AI-based tool "Nuha"[32] (Arabic for "mind" or "brain") to help researchers and civil society organisations detect online gender-based violence and hate speech in Jordanian Arabic, especially on social media platforms. "Despite challenges such as data imbalance and Twitter API limitations, Nuha achieves a 72 percent F1 score in identifying hate speech, reflecting its effectiveness", according to a 2023 report on the project by DRI (Democracy Reporting International 2023: 11).

Beyond data availability, one of the key challenges in terms of cybercrime (legislation) is the interdisciplinary nature of the issue, "with traditional boundaries preventing researchers gaining a comprehensive understanding of cybercrime, including technical, legal, and social aspects" (Hansel and Silomon, 2023: 29). To better tackle cybercrime and unintended harmful effects related to cybercrime legislation, **states should financially support research that combines "different and dispersed silos of knowledge as well as research methodologies" (ibid.) and multistakeholder cooperation**, e.g. between academia and (feminist) civil society.

[32] The AI model is publicly available here: http://nuha.josa.ngo/.

BIBLIOGRAPHY

Access Now 2015, Implementation Guide for the International Principles on the Application of Human Rights to Communications Surveillance, viewed 12 February 2025, https://necessaryandproportionate.org/files/implementation_guide_international_principles_2015.pdf.

Access Now 2018, Statement opposing Egypt's legalization of website blocking and communications surveillance, viewed 12 February 2025, https://www.accessnow.org/press-release/statement-opposing-egypts-legalization-of-website-blocking-and-communications-surveillance-2/.

Access Now 2024, Oral Statement – UN Ad Hoc Committee on Cybercrime Reconvened Concluding Session 30 July 2024, viewed 13 February 2025, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP8/Oral_Statement_-_UN_Ad_Hoc_Committee_on_Cybercrime_Reconvened_Concluding_Session_30_July_2024.pdf.

Access Now n.d., Digital Security Helpline, viewed 12 February 2025, https://www.accessnow.org/help/.

Adams, A.C. & Podair, D. 2024, ‚Confusion & Contradiction in the UN "Cybercrime" Convention', Lawfare, viewed 13 February 2025, https://www.lawfaremedia.org/article/confusion--contradiction-in-the-un-cybercrime--convention.

AFP 2024, Nicaragua's new legal reforms target opponents and critics, viewed 12 February 2025, https://ticotimes.net/2024/10/05/nicaraguas-new-legal-reforms-target-opponents-and-critics.

Africanews 2023, Libya: HRW asks to repeal a law on cybercrime, viewed 12 February 2025, https://www.africanews.com/2023/04/04/libya-hrw-asks-to-repeal-a-law-on-cybercrime/.

AHC 2021, Proposed Outline and Modalities for the Ad Hoc Committee on Cybercrime Conference room paper submitted by Australia, Canada, Chile, the Dominican Republic, Honduras, Japan, New Zealand, Norway, the United Kingdom and the United States of America, status date 4 December 2020, A/AC.291/CRP.1, viewed 13 February 2025, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/CRPs/V2100299.pdf.

Al Sur 2024, Al Sur's open letter on international convention cybercrime, viewed 13 February 2025, https://www.alsur.lat/en/blog/alsurs-open-letter-international-convention-cybercrime.

Allinson, T. 2020, ‚Egypt's rising #MeToo movement dealt blow', DW, viewed 12 February 2025, https://www.dw.com/en/setback-to-egypts-metoo-movement-as-rape-witnesses-reportedly-charged/a-54958956.

Amnesty International 2018, Crowdsourced Twitter study reveals shocking scale of online abuse against women, viewed 12 February 2025, https://www.amnesty.org/en/latest/press-release/2018/12/crowdsourced-twitter-study-reveals-shocking-scale-of-online-abuse-against-women/.

Amnesty International 2021, Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, viewed 12 February 2025, https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/.

Amnesty International 2022, Tunisia: Repeal Draconian Cybercrime Decree, viewed 12 February 2025, https://www.amnesty.org/en/documents/mde30/6290/2022/en/.

Amnesty International 2023, Jordan's new proposed cybercrimes law will strongly undermine digital rights, viewed 13 February 2025, https://www.amnesty.org/en/documents/mde16/7053/2023/en/.

Amnesty International 2024a, The State of the World's Human Rights: April 2024, viewed 11 February 2025, https://www.amnesty.org/en/documents/pol10/7200/2024/en/.

Amnesty International 2024b, Jordan: New Cybercrimes Law stifling freedom of expression one year on, viewed 12 February 2025, https://www.amnesty.org/en/latest/news/2024/08/jordan-new-cybercrimes-law-stifling-freedom-of-expression-one-year-on/.

Amnesty International 2024c, Jordan: New Cybercrimes Law stifles freedom of expression, viewed 12 February 2025, https://www.amnesty.org/en/documents/mde16/8424/2024/en/.

AP News 2020, Nicaragua approves "cybercrimes" law, alarming rights groups, viewed 12 February 2025, https://apnews.com/general-news-ce252ed4721a759ed329798a7e2e30db.

AP News 2024, Tunisian commentator sentenced to two years under controversial anti-fake news law, viewed 12 February 2025, https://apnews.com/article/tunisia-dahmani-decree-54-misinformation-crackdown-dissent-5d1cd879bb081796439a469db744014e.

Article 19 2023, Tunisia: Decree-law No 54 of 2022, viewed 13 February 2025, https://www.article19.org/wp-content/uploads/2023/03/Analysis-of-decree-law-54-English.pdf.

Association for Progressive Communications 2023, A framework for developing gender-responsive cybersecurity policy: Assessment tool, viewed 12 February 2025, https://www.apc.org/en/pubs/framework-developing-gender-responsive-cybersecurity-policy-assessment-tool.

Bada, M., Chua, Y.T., Collier, B. & Pete, I. 2021, ‚Cybersecurity and cybercrime: rethinking threats and responses', in M. Christen, B. Gordijn & M. Loi (eds), The ethics of cybersecurity, The International Library of Ethics, Law and Technology, vol. 21, Springer, Cham, pp. 263–283, viewed 12 February 2025, https://doi.org/10.1007/978-3-030-60527-8_14.

BBC News 2024, Europe facing ‚wave of antisemitism', survey finds, viewed 13 February 2025, https://www.bbc.com/news/articles/c147w9572dvo.

Benshimon, S. 2024, ‚Tunisie: Sonia Dahmani, avocate et chroniqueuse, condamnée à deux ans de prison', Sahel Intelligence, viewed 12 February 2025, https://sahel-intelligence.com/35554-tunisie-sonia-dahmani-avocate-et-chroniqueuse-condamnee-a-deux-ans-de-prison.html.

Bernarding, N. & Kobel, V. 2023, ‚Feminist Perspectives on the Militarisation of Cyberspace', Centre for Feminist Foreign Policy, viewed 12 February 2025, https://centreforfeministforeignpolicy.org/wordpress/wp-content/uploads/2023/06/CFFP_Briefing_Cybersecurity_final.pdf.

Bhandari, V. & Kovacs, A. 2021, ‚What's sex got to do with it? Mapping the impact of questions of gender and sexuality on the evolution of the digital rights landscape in India', Internet Democracy Project, viewed 12 February 2025,https://cdn.internetdemocracy.in/idp/assets/downloads/reports/whats-sex-got-to-do-with-it-mapping-the-impact-of-questions-of-gender-and-sexuality-on-the-evolution-of-the-digital-rights-landscape-in-india/Vrinda-Bhandari-and-Anja-Kovacs-Whats-Sex-Got-To-Do-with-It.pdf.

Boutry, T. 2024, ‚Tunisie : une avocate et chroniqueuse condamnée à 8 mois de prison en appel pour avoir critiqué le pays', Le Parisien, viewed 12 February 2025, https://www.leparisien.fr/international/tunisie-une-avocate-et-chroniqueuse-condamnee-a-8-mois-de-prison-en-appel-pour-avoir-critique-le-pays-11-09-2024-RMEPBERTQBDTRHFKYOHOD6CNWY.php.

Centre for Feminist Foreign Policy 2021, The CFFP Glossary, viewed 13 February 2025, https://centreforfeminist-foreignpolicy.org/2021/03/08/feminist-glossary-2/.

Chatham House 2022, Gender mainstreaming and the proposed cybercrime convention: Commentary on the consolidated draft, viewed 13 February 2025, https://www.chathamhouse.org/sites/default/files/2022-12/2022-12-21-Gender-mainstreaming-and-the-proposed-cybercrime-convention.pdf.

Chatham House 2023, Integrating gender in cybercrime capacity-building: a toolkit, viewed 13 February 2025, https://www.chathamhouse.org/sites/default/files/2023-07/2023-07-05-integrating-gender-in-cybercrime-capacity-building-emerson-keeler-et-al.pdf.

Chatham House n.d., How can the cybercrime convention adopt a strategic approach to cybercrime capacity building and protect against potential harms and misuses?, viewed 13 February 2025, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/Multi-stakeholders/Chatham_House.pdf.

Civicus Monitor 2023, Draconian cybercrime law used to target protesters, HRDs, journalists amid pro-Palestine protests, viewed 13 February 2025, https://monitor.civicus.org/explore/draconian-cybercrime-law-used-to-target-protesters-hrds-journalists-amid-pro-palestine-protests/.

Columbia University n.d., 'Nyanzi v. Uganda', Global Freedom of Expression, viewed 12 February 2025, https://globalfreedomofexpression.columbia.edu/cases/case-dr-stella-nyanzi/.

Council of Europe 2021, Protecting women and girls from violence in the digital age: the relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women, viewed 12 February 2025, https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3.

Council of Europe 2022, The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform: Thematic paper of the Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW), viewed 13 February 2025, https://www.ohchr.org/sites/default/files/documents/hrbodies/cedaw/statements/2022-12-02/EDVAW-Platform-thematic-paper-on-the-digital-dimension-of-VAW_English.pdf.

Council on Foreign Relations 2024, Abortion Law: Global Comparisons, viewed 13 February 2025, https://www.cfr.org/article/abortion-law-global-comparisons.

Creutzfeldt, N., Kyprianides, A., Bradford, B. & Jackson, J. 2024, ‚Marginalized groups and unmet legal needs', in Access to justice, digitalization and vulnerability: exploring trust in justice, Policy Press, Bristol, viewed 12 February 2025, https://doi.org/10.1332/policypress/9781529229523.003.0009.

Cybersecurity Tech Accord 2024a, Cybersecurity Tech Accord Statement to Reconvened concluding session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, viewed 13 February 2025, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Cybersecurity_Tech_Accord_Statement_07.30_AHC7.13.pdf.

Cybersecurity Tech Accord 2024b, Cybersecurity Tech Accord Submission to the Concluding Session of the Ad Hoc Committee to Elaborate a UN Convention on Countering Cybercrime, viewed 13 February 2025, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Multi-Stakeholders/Cybersecurity_Tech_Accord_-_7th_AHC_session_submission.pdf.

Democracy Reporting International 2023, Online public discourse in the MENA region: Anti-immigrant hate speech, AI solutions, detecting online violence against women, and regional strategies, viewed 13 February 2025, https://democracy-reporting.org/en/office/global/publications/online-public-discourse-in-the-mena-region-persistent-tactics-of-disinformation-and-an-increase-in-online-gender-based-violence.

Derechos Digitales 2023, Human rights in digital environments in Nicaragua, viewed 12 February 2025, https://www.derechosdigitales.org/nicaragua-2023-eng/.

Derechos Digitales & Association for Progressive Communications 2023, When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks, viewed 12 February 2025, https://www.apc.org/en/pubs/when-protection-becomes-excuse-criminalisation-gender-considerations-cybercrime-frameworks.

Digital Rights Foundation n.d., Cyber Harassment Helpline, viewed 12 February 2025, https://digitalrightsfoundation.pk/cyber-harassment-helpline/.

Egypt 2018, Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes, WIPO Lex, viewed 13 February 2025, https://www.wipo.int/wipolex/en/legislation/details/19959.

EPICenter Works n.d., Joint letter to EU and member states on UN Cybercrime Convention, viewed 13 February 2025, https://epicenter.works/fileadmin/user_upload/Joint_letter_to_EU_and_member_states_on_UN_Cybercrime_Convention.pdf.

Freedom House 2024, Freedom on the Net 2024: The Struggle for Trust Online, viewed 11 February 2025, https://freedomhouse.org/report/freedom-net/2024/struggle-trust-online.

Freedom Online Coalition 2024, FOC Advisory Network Proactive Advice on UN Convention Against Cybercrime, viewed 13 February 2025, https://freedomonlinecoalition.com/foc-advisory-network-proactive-advice-un-convention-against-cybercrime/.

Gavrilovic Nilsson, M., Tzani Pepelasi, K., Ioannou, M. & Lester, D. 2019, ‚Understanding the link between sextortion and suicide', International Journal of Cyber Criminology, vol. 13, no. 1, pp. 55–69, viewed 12 February 2025, https://pure.hud.ac.uk/en/publications/understanding-the-link-between-sextortion-and-suicide.

Ghai, Y. & Cottrell, J. (eds) 2009, Marginalized Communities and Access to Justice, Routledge, London, viewed 12 February 2025, https://worldjusticeproject.org/our-work/publications/edited-volumes/marginalized-communities-and-access-justice.

GenderIT.org 2008, Cybercrime legislation and gender, viewed 12 February 2025, https://www.genderit.org/edition/cybercrime-legislations-and-gender.

GenderIT.org 2018, 13 Manifestations of Gender-Based Violence Using Technology, viewed 13 February 2025, https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology.

Gollan, J. 2023, ‚Websites Selling Abortion Pills Are Sharing Sensitive Data With Google', Ms. Magazine, viewed 13 February 2025, https://msmagazine.com/2023/01/18/google-abortion-pills-privacy-data/.

Gullo, K. 2024, Protect Good Faith Security Research Globally in Proposed UN Cybercrime Treaty, Electronic Frontier Foundation, viewed 13 February 2025, https://www.eff.org/deeplinks/2024/02/protect-good-faith-security-research-globally-proposed-un-cybercrime-treaty.

Hakmeh, J. & Saunders, J. 2024, The Strategic Approach to Countering Cybercrime (SACC) Framework, Chatham House, London, viewed 12 February 2025, https://www.chathamhouse.org/sites/default/files/2024-07/2024-07-11-strategic-approach-countering-cybercrime-framework-hakmeh-saunders.pdf.

Hakmeh, J. 2024, ‚The UN convention on cybercrime: a milestone in cybercrime cooperation?', Journal of Cyber Policy, vol. 9, no. 2, pp. 125–130, viewed 13 February 2025, https://doi.org/10.1080/23738871.2024.2441549.

Hassan, Z. & Hellyer, H.A. 2024, Suppressing Dissent: Shrinking Civic Space, Transnational Repression and Palestine–Israel, Carnegie Endowment for International Peace, viewed 13 February 2025, https://carnegieendowment.org/research/2024/10/suppressing-dissent-shrinking-civic-space-transnational-repression-and-palestine-israel?lang=en.

Human Rights Foundation 2017, Uganda: Drop "Cyber-Harassment" Charges Against Activist for Facebook Posts, viewed 12 February 2025, https://archive.hrf.org/press-release-uganda-drop-cyber-harassment-charges-against-activist-for-facebook-posts/.

Human Rights Watch 2020, Egypt: Spate of "Morality" prosecutions of women, viewed 12 February 2025, https://www.hrw.org/news/2020/08/17/egypt-spate-morality-prosecutions-women.

Human Rights Watch 2021, Abuse of cybercrime measures taints UN talks, viewed 12 February 2025, https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks.

Human Rights Watch 2023a, Libya: revoke repressive anti-cybercrime law, viewed 12 February 2025, https://www.hrw.org/news/2023/04/03/libya-revoke-repressive-anti-cybercrime-law.

Human Rights Watch 2023b, Tunisia: cybercrime decree used against critics, viewed 12 February 2025, https://www.hrw.org/news/2023/12/19/tunisia-cybercrime-decree-used-against-critics.

Human Rights Watch 2023c, "All This Terror Because of a Photo": Digital Targeting and Its Offline Consequences for LGBT People in the Middle East and North Africa, viewed 13 February 2025, https://www.hrw.org/report/2023/02/21/all-terror-because-photo/digital-targeting-and-its-offline-consequences-lgbt.

Human Rights Watch 2024a, Uganda: Court Upholds Anti-Homosexuality Act, viewed 12 February 2025, https://www.hrw.org/news/2024/04/04/uganda-court-upholds-anti-homosexuality-act.

Human Rights Watch 2024b, Jordan: Arrests, Harassment of Pro-Palestine Protesters, viewed 12 February 2025, https://www.hrw.org/news/2024/02/06/jordan-arrests-harassment-pro-palestine-protesters.

Human Rights Watch 2024c, Russia: First Convictions Under LGBT "Extremist" Ruling, viewed 12 February 2025, https://www.hrw.org/news/2024/02/15/russia-first-convictions-under-lgbt-extremist-ruling.

Human Rights Watch 2024d, Upcoming cybercrime treaty will be nothing trouble, viewed 13 February 2025, https://www.hrw.org/news/2024/08/07/upcoming-cybercrime-treaty-will-be-nothing-trouble.

Hu, Y., Chen, X. & Bose, I. 2013, ‚Cybercrime enforcement around the globe', Journal of Information Privacy and Security, vol. 9, no. 3, pp. 34–52, viewed 12 February 2025, https://doi.org/10.1080/15536548.2013.10845684.

Hollingworth, D. 2024, ‚Tech companies call for changes to draft UN Cybercrime Convention', Cyber Daily, viewed 13 February 2025, https://www.cyberdaily.au/security/10895-tech-companies-call-for-changes-to-draft-un-cybercrime-convention.

International Association of Women Judges n.d., Naming, shaming, ending sextortion: A Toolkit, viewed 13 February 2025, https://www.unodc.org/res/ji/import/guide/naming_shaming_ending_sextortion/naming_shaming_ending_sextortion.pdf.

International Chamber of Commerce 2024, Global business urges governments to reject new international cybercrime treaty, viewed 13 February 2025, https://iccwbo.org/news-publications/news/global-business-urges-governments-to-reject-new-international-cybercrime-treaty/.

International Telecommunication Union 2023, Population of global offline continues steady decline to 2.6 billion people in 2023, viewed 12 February 2025, https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx.

International Telecommunication Union 2024, Measuring Digital Development: Facts and Figures 2024, viewed 12 February 2025, https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-4/.

Jain, G. 2024, ‚From buttocks to electronic bracelets: How governments are using cybercrime laws to target women and LGBTQIA+ people', Association for Progressive Communications, viewed 13 February 2025, https://www.apc.org/en/news/buttocks-electronic-bracelets-how-governments-are-using-cybercrime-laws-target-women-and.

Jbour, A. 2023, ‚Jeopardizing digital rights in Jordan', Carnegie Endowment for International Peace, viewed 12 February 2025, https://carnegieendowment.org/sada/2023/08/jeopardizing-digital-rights-in-jordan?lang=en.

Jordan Prime Minister's Office 2023, إعلان صدور قانون رقم 17 لسنة 2023 لمكافحة الجرائم الإلكترونية [Jordan's new Law No. 17 of 2023 on Combating Cybercrimes], viewed 13 February 2025, https://perma.cc/7RSM-6S4K.

Juma, A. & Knipp, K. 2020, ‚Egypt imprisons female TikTok influencers', DW, viewed 12 February 2025, https://www.dw.com/en/egyptian-tiktok-stars-jailed/a-54371869.

Kävrestad, J., Birath, M. & Clarke, N. 2024, ‚Cyber-Dependent Crime, Cyber-Enabled Crime, and Digital Evidence', in Fundamentals of Digital Forensics, Texts in Computer Science, Springer, Cham, viewed 12 February 2025, https://doi.org/10.1007/978-3-031-53649-6_6.

Kataeva, Z., Durrani, N., Izekenova, Z. & Roshka, V. 2024, ‚Thirty years of gender mainstreaming: Evolution, development, and future research agenda through a bibliometric approach', Women's Studies International Forum, vol. 107, viewed 13 February 2025, https://doi.org/10.1016/j.wsif.2024.103010.

La Presse 2024, Décret loi n°54 : Sonia Dahmani condamnée à un an de prison, viewed 12 February 2025, https://lapresse.tn/2024/07/06/decret-loi-n54-sonia-dahmani-condamnee-a-un-an-de-prison/.

Leukfeldt, E.R., Notté, R.J. & Malsch, M. 2019, ‚Exploring the needs of victims of cyber-dependent and cyber-enabled crimes', Victims & Offenders, vol. 15, no. 1, pp. 60–77, viewed 12 February 2025, https://doi.org/10.1080/15564886.2019.1672229.

Lima, V. & Gomez, M. 2021, ‚Access to Justice: Promoting the Legal System as a Human Right', in Leal Filho, W, Marisa Azul, A, Brandli, L, Lange Salvia, A, Özuyar, P.G & Wall, T (eds), Peace, Justice and Strong Institutions. Encyclopedia of the UN Sustainable Development Goals, Springer, Cham, viewed 13 February 2025, https://doi.org/10.1007/978-3-319-95960-3_1.

Libya 2022, Law No. 5 of 2022 regarding Combating Cybercrimes, The Law Society of Libya, viewed 13 February 2025, https://lawsociety.ly/en/legislation/law-no-5-of-2022-regarding-combating-cybercrimes/.

McCubbin, J. 2024, ‚Sextortion: The deadly scam targeting young men', BBC News, viewed 12 February 2025, https://www.bbc.com/news/articles/cq82lyg5vpjo.

McGuire, M. & Dowling, S. 2013, Cyber crime: A review of the evidence: Research Report 75 - Summary of key findings and implications, UK Home Office, viewed 13 February 2025, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf.

Makooi, B. 2023, ‚Egypt's female social media influencers face arrest, jail on „morality" charges', France 24, viewed 12 February 2025, https://www.france24.com/en/middle-east/20230411-egypt-s-female-social-media-influencers-face-arrest-jail-on-morality-charges.

Maimon, D. & Louderback, E.R. 2019, ‚Cyber-Dependent Crimes: An Interdisciplinary Review', Annual Review of Criminology, vol. 2, no. 1, pp. 191–216, viewed 12 February 2025, https://doi.org/10.1146/annurev-criminol-032317-092057.

Mendel, T. n.d., ‚Freedom of expression: a guide to the interpretation and meaning of Article 10 of the European Convention on Human Rights', Council of Europe, viewed 12 February 2025, https://rm.coe.int/16806f5bb3.

Microsoft 2024, Cybercrime Convention Negotiations Microsoft's submission to the Seventh Reconvened Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, viewed 13 February 2025, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP9/Microsoft_-_Reconvened_Substantive_Session.pdf.

Miranda Aburto, W. 2024, ‚Nicaragua tightens control of social media to censor dissent', El País, viewed 12 February 2025, https://english.elpais.com/international/2024-09-12/nicaragua-tightens-control-of-social-media-to-censor-dissent.html.

Mwesigwa, A. 2017, ‚Jailed for calling Ugandan president a „pair of buttocks", activist vows to fight on', The Guardian, viewed 12 February 2025, https://www.theguardian.com/global-development/2017/jun/19/jailed-for-calling-ugandan-president-museveni-a-pair-of-buttocks-activist-vows-to-fight-on-stella-nyanzi.

Nord, M., Lundstedt, M., Altman, D., Angiolillo, F., Borella, C., Fernandes, T., Gastaldi, L., Good God, A., Natsika, N. & Lindberg, S.I. 2024, Democracy Report 2024: Democracy Winning and Losing at the Ballot, V-Dem Institute, University of Gothenburg, viewed 12 February 2025, https://v-dem.net/documents/43/v-dem_dr2024_lowres.pdf.

OMCT 2021, Nicaragua: criminalización de Amaru Ruiz Alemán, viewed 12 February 2025, https://www.omct.org/es/recursos/llamamientos-urgentes/nicaragua-criminalizaci%C3%B3n-de-amaru-ruiz-alem%C3%A1n.

OHCHR 2018, 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, A/HRC/38/47, viewed 12 February 2025, https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and.

Palassis, A., Speelman, C.P. & Pooley, J.A. 2021, ‚An Exploration of the Psychological Impact of Hacking Victimization', SAGE Open, vol. 11, no. 4, pp. 1–12, viewed 12 February 2025, https://doi.org/10.1177/21582440211061556.

Pavlova, P. 2024, Gendered Harms of Data Weaponization: Historical Patterns, New Battlefields, and the Implications for Democracy and National Security, New America, viewed 12 February 2025, https://www.newamerica.org/future-security/reports/gendered-harms-of-data-weaponization/.

Penal Reform International 2012, Access to Justice: Discrimination of Women in Criminal Justice Systems, viewed 12 February 2025, https://cdn.penalreform.org/wp-content/uploads/2013/08/BRIEFING-Discrimination-women-criminal-justice.pdf.

ProtectDefenders.eu 2021, Nicaragua: harassment and killings of human rights defenders, viewed 12 February 2025, https://protectdefenders.eu/nicaragua-harassment-and-killings-of-human-rights-defenders/.

RadioFreeEurope/RadioLiberty 2021, Afghan women move protests to social media to evade violent Taliban response, viewed 12 February 2025, https://www.rferl.org/a/afghanistan-women-rights-protests-taliban/31598129.html.

Revenge Porn Helpline n.d., South West Grid for Learning (SWGfL), viewed 12 February 2025, https://swgfl.org.uk/research/revenge-porn-helpline-annual-report/.

Rigot, A. 2020, ‚Egypt's economic courts are being used to target LGBTQ people', Slate, viewed 12 February 2025, https://slate.com/technology/2020/12/egypt-lgbtq-crime-economic-courts.html.

Rodriguez, K. 2024, ‚EFF's Concerns About the UN Draft Cybercrime Convention', Electronic Frontier Foundation, viewed 13 February 2025, https://www.eff.org/deeplinks/2024/07/effs-concerns-about-un-draft-cybercrime-convention.

Robalo, T.L.A.S. & Abdul Rahim, R.B.B. 2023, ‚Cyber Victimisation, Restorative Justice and Victim-Offender Panels', Asian Journal of Criminology, vol. 18, no. 1, pp. 61–74, viewed 12 February 2025, https://doi.org/10.1007/s11417-023-09396-9.

Sarre, R, Lau, L.Y-C & Chang, L.Y.C. 2018, ‚Responding to cybercrime: current trends', Police Practice and Research, vol. 19, no. 6, pp. 515–518, viewed 12 February 2025, https://doi.org/10.1080/15614263.2018.1507888.

Scher-Zagier, E. 2024, ‚The New UN Cybercrime Treaty Is a Bigger Deal Than Even Its Critics Realize', Lawfare, viewed 13 February 2025, https://www.lawfaremedia.org/article/the-new-un-cybercrime-treaty-is-a-bigger-deal-than-even-its-critics-realize.

Seitenova, A., Kobel, V. & Bernarding, N. 2024, Strongmen and Violence: Interlinkages of Anti-Feminism and Anti-Democratic Developments, Centre for Feminist Foreign Policy, viewed 13 February 2025, https://centreforfeministforeignpolicy.org/wordpress/wp-content/uploads/2024/02/CFFP-strongmen-and-violence.pdf.

Shires, J., Hassib, B. & Swali, A. 2024, Gendered Hate Speech, Data Breach, and State Overreach: Identifying the Connections Between Gendered Cyber Harms to Shape Better Policy Responses, Chatham House, viewed 12 February 2025, https://www.chathamhouse.org/sites/default/files/2024-05/2024-05-24-gendered-cyber-harms-shires-et-al_0.pdf.

Smith, T. & Crawford, A. 2024, ‚Sextortion guides sold on social media, BBC finds', BBC News, viewed 12 February 2025, https://www.bbc.com/news/articles/cp00y03q93mo.

SMEX n.d., Digital Safety Helpdesk, viewed 12 February 2025, https://smex.org/helpdesk/.

StopNCII.org n.d., Stop Non-Consensual Intimate Image Abuse, viewed 12 February 2025, https://stopncii.org/.

Stock, E. 2021, ‚Two new laws intensify the crackdown on journalists in Nicaragua', International Center for Journalists, viewed 12 February 2025, https://www.icfj.org/news/two-new-laws-intensify-crackdown-journalists-nicaragua.

SWGfL n.d., Intimate image abuse: an evolving landscape, SWGfL, viewed 12 February 2025, https://revenge-pornhelpline.org.uk/assets/documents/intimate-image-abuse-an-evolving-landscape.pdf.

Tennant, I. & Oliveira, A.P. 2024, ‚Applying the right lessons from the negotiation and implementation of the UNTOC and the UNCAC to the implementation of the newly agreed UN "cybercrime" treaty', Journal of Cyber Policy, vol. 9, no. 2, pp. 221–238, viewed 13 February 2025, https://doi.org/10.1080/23738871.2024.2428655.

The Independent 2023, Law that criminalised Stella Nyanzi, Kakwenza kicked out, viewed 12 February 2025, https://www.independent.co.ug/law-that-criminalised-stella-nyazi-kakwenza-kicked-out/.

The New Arab 2023, Egyptian model sentenced to 2 years in jail for "debauchery", viewed 12 February 2025, https://www.newarab.com/news/egyptian-model-sentenced-2-years-jail-debauchery.

The New York Times 2023, Antisemitic and Anti-Muslim Hate Speech Surges Across the Internet, viewed 13 February 2025, https://www.nytimes.com/2023/11/15/technology/hate-speech-israel-gaza-internet.html.

Tidy, J. 2024, ‚Dead in 6 hours: How Nigerian sextortion scammers targeted my son', BBC News, viewed 12 February 2025, https://www.bbc.com/news/articles/c2llzppyx05o.

Treaty on the Functioning of the European Union [2008] OJ C115/47, art 218(11), Official Journal of the European Union, viewed 12 February 2025, https://eur-lex.europa.eu/eli/treaty/tfeu_2008/art_218/oj/eng.

Tunisia 2022, Décret Loi n°2022-54 du 13 septembre 2022 relatif à la lutte contre les infractions se rapportant aux systèmes d'information et de communication, DCAF, viewed 13 February 2025, https://legislation-securite.tn/latest-laws/decret-loi-n-2022-54-du-13-septembre-2022-relatif-a-la-lutte-contre-les-infractions-se-rapportant-aux-systemes-dinformation-et-de-communication/.

Uganda 2011, The Computer Misuse Act, Government of Uganda, viewed 13 February 2025, https://commons.laws.africa/akn/ug/act/2011/2/media/publication/ug-act-2011-2-publication-document.pdf.

United Nations General Assembly 2021, Promotion and protection of the right to freedom of opinion and expression, A/76/258, viewed 12 February 2025, https://documents.un.org/doc/undoc/gen/n21/212/16/pdf/n2121216.pdf.

United Nations General Assembly 2024a, Resolution 79/243: United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, viewed 11 February 2025, https://documents.un.org/access.nsf/get?DS=A/RES/79/243&Lang=E.

United Nations General Assembly 2024b, Global threats to freedom of expression arising from the conflict in Gaza, United Nations, viewed 13 February 2025, https://documents.un.org/doc/undoc/gen/n24/247/88/pdf/n2424788.pdf.

United Nations Human Rights Committee 2011, General comment no. 34: Article 19: freedoms of opinion and expression, CCPR/C/GC/34, viewed 12 February 2025, https://documents.un.org/doc/undoc/gen/g11/453/31/pdf/g1145331.pdf.

United Nations Human Rights Council 2019a, Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/41/35, viewed 12 February 2025, https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur.

United Nations Human Rights Council 2019b, Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/HRC/40/52, viewed 12 February 2025, https://docs.un.org/en/A/HRC/40/52.

United Nations Human Rights Council 2020, Report of the Special Rapporteur on the right to privacy, A/HRC/43/52, viewed 12 February 2025, https://documents.un.org/doc/undoc/gen/g20/071/66/pdf/g2007166.pdf.

United Nations High Commissioner for Human Rights 2018, The Right to Privacy in the Digital Age, A/HRC/39/29, United Nations, viewed 12 February 2025, https://digitallibrary.un.org/record/1640588/files/A_HRC_39_29-EN.pdf?ln=en.

United Nations High Commissioner for Human Rights n.d., Information Note: Human rights and the draft Cybercrime Convention, viewed 13 February 2025, https://www.ohchr.org/sites/default/files/documents/issues/civicspace/DRAFT-CYBERCRIME-CONVENTION.pdf.

UN News 2024, UN adopts landmark convention to combat cybercrime, viewed 11 February 2025, https://news.un.org/en/story/2024/12/1158521.

UNODC n.d., Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, viewed 13 February 2025, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

UNODC n.d., University Module Series: Cybercrime - Module 2: General Types of Cybercrime, viewed 13 February 2025, https://www.unodc.org/e4j/en/cybercrime/module-2/index.html.

UNODC n.d., SHERLOC – Database on Cybercrime Legislation, viewed 12 February 2025, https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#?c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23__el.legislation.crimeTypes_s%22,%22value%22:%22Cybercrime%22%7D%5D,%22sortings%22:%22%22%7D.

UNODC 2023, Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, viewed 13 February 2025, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf.

UNRIC 2024, Cyberviolence against women and girls: the growing threat of the digital age, viewed 12 February 2025, https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/.

UN Women n.d., Libya, viewed 12 February 2025, https://arabstates.unwomen.org/en/countries/libya.

U.S. Attorney's Office, Southern District of Indiana 2023, FBI and partners issue national public safety alert on sextortion schemes, viewed 12 February 2025, https://www.justice.gov/usao-sdin/pr/fbi-and-partners-issue-national-public-safety-alert-sextortion-schemes.

Uhlich, M., Tan, R.K.J., Azevedo, V. et al. 2024, ‚Online harassment during COVID-19: a cross-sectional analysis across 10 countries from the I-SHARE consortium', Journal of Public Health (Berl.), viewed 12 February 2025, https://doi.org/10.1007/s10389-024-02332-w.

Walker, S. & Oliveira, A.P. 2024a, ‚The final call: UN member states adopt a new cybercrime treaty', Global Initiative Against Transnational Organized Crime, viewed 13 February 2025, https://globalinitiative.net/wp-content/uploads/2024/09/Summer-Walker-Ana-Paula-Oliveira-The-final-call-UN-member-states-adopt-a-new-cybercrime-treaty-GI-TOC-September-2024.pdf.

Walker, S. & Oliveira, A.P. 2024b, ‚The Final Call: UN Member States Adopt a New Cybercrime Treaty', Global Initiative Against Transnational Organized Crime, viewed 13 February 2025, https://globalinitiative.net/analysis/the-final-call-un-member-states-adopt-a-new-cybercrime-treaty/.

Wong, O. 2024, Cyberwarfare: The ‚Pink Tax' of Hacking, Centre for International and Defence Policy, Queen's University, Kingston, Ontario, viewed 13 February 2025, https://www.queensu.ca/cidp/sites/cidpwww/files/uploaded_files/9-2%20CIDP%20-%20PolicyBrief%20Owen%20Wong%20Apr2024.pdf.

Wright, D. 2024, ‚A Global Framework for Change: Discussing NCII at the UN Cybercrime Convention', SWGfL, viewed 13 February 2025, https://swgfl.org.uk/magazine/a-global-framework-for-change-discussing-ncii-at-the-un-cybercrime-convention/.

Zaghdoudi, A. 2023, Freedom of Expression at risk in Tunisia: a legal framework that favors silence, Access Now, viewed 12 February 2025, https://www.accessnow.org/wp-content/uploads/2023/05/FoE-Report-English-Final.pdf.

Victim Support n.d., viewed 12 February 2025, https://www.victimsupport.org.uk/.