APC POLICY EXPLAINERS

APC POLICY EXPLAINER: CYBERCRIME AND GENDER

What is a gender approach to cybercrime?

The problem

The change we want to see

How APC works on this issue

Where is the discussion taking place?

Some spaces to engage with

Some organisations working on this issue

Read more

Coordination and editing: Verónica Ferrari and Paula Martins (APC)
Proofreading: Lori Nordstrom (APC)
Design and layout: Cathy Chen (APC)
APC would like to thank Maia Levy Daniel, an external researcher,
who supported the development of this explainer.

WHAT IS A GENDER APPROACH TO CYBERCRIME?

While cybercrime laws could be seen as necessary to protect human rights, both in the digital and analogue realms, they may also be used as tools to legitimise surveillance and censorship of historically excluded groups, and may heighten pre-existing structural inequalities.

In order to effectively protect human rights, cybercrime norms should be carefully drafted, ensuring safeguards and protections in alignment with international human rights standards.

Taking a gender approach into account is also important. Much of digital criminality disproportionately targets women and gender non-conforming persons. Looking at cybercrime from a gender lens means to recognise and take into account the lived experiences of women and people of diverse sexualities and gender expressions, to understand their needs and priorities, and address the differentiated impacts of cybercrime on the basis of gender in conjunction with other intersectionalities.

THE PROBLEM

States have international obligations to act diligently to protect the rights of people in digital spaces, and this is particularly important for historically excluded groups, such as women and LGBTQIA+ people, whose rights are threatened both online and offline.

Women and gender-diverse people still face two major challenges in the online space: the gender gap (and other digital divides) remains a reality for large numbers of women and gender-diverse individuals and, when they manage to connect, too often they are subjected to harassment, discrimination and violence, also known as technology-facilitated gender-based violence (TFGBV).

According to the United Nations Population Fund (UNFPA), "technology-facilitated gender-based violence, or TFGBV, is an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person on the basis of their gender." TFGBV results in or is likely to result in physical, sexual, psychological, social, political or economic harm or other infringements of rights and freedoms.

Cybercrime may have different impacts on different groups. For instance, ransomware attacks on health care systems could be particularly harmful for women and other marginalised groups because of societal discrimination. Thus, when these aspects are not taken into account, solutions such as cybercrime laws are

ultimately ineffective and disproportionate, and can put those they intend to protect at risk .

Cybercrime laws that do not take gender into account ignore important differences in the capabilities, needs and priorities of women in all their diversity, LGBTQI+ people and other historically excluded groups when they operate within the criminal justice system and/or experience vulnerability to cybercrime. Without a gender intersectional perspective, pre-existing structural inequalities may be aggravated and perpetuated by digital technologies and the laws and norms that govern them.

Moreover, broad regulations with vaguely typified conducts may facilitate discretional interpretation and implementation, legitimising cyber surveillance and censorship in certain contexts. In different parts of the world, it is possible to find abusive use of national cybercrime legislation as a tool to undermine human rights and criminalise legitimate activities, targeting civil society organisations, human rights defenders, digital security researchers, whistleblowers and journalists. Cybercrime legislation has also been used to silence dissent and women who want to speak up, to threaten freedom of expression, and to validate state surveillance.

This is why advancing international standards on cybercrime without considering the diversity of national contexts or safeguards for the protection of human rights, particularly of historically marginalised groups, is dangerous.

THE CHANGE WE WANT TO SEE

There is a need to include gender perspectives in cybercrime discussions and regulations to avoid exacerbating inequalities that affect historically excluded groups such as women and LGBTQIA+ people. A gender perspective may address the specific needs and priorities of women and people of diverse sexualities and gender expressions and the differentiated impacts of cybercrime on the basis of gender in conjunction with other intersectionalities.

In this regard, it is relevant to stress that in the most recent UN General Assembly resolution (A/RES/77/211) on the right to privacy in the digital age, the assembly recognises the importance of the promotion of and respect for the right to privacy as a way to prevent gender-based violence as well as any form of discrimination that can occur in digital and online spaces. In the same resolution, the assembly encourages states to mainstream a gender perspective in the conceptualisation, development and implementation of digital technologies and related policies.

A gender analysis of the cybercrime landscape helps to identify risks and harms that can be gender-disaggregated. Gender should be mainstreamed in order to make every person's concerns and experiences an integral dimension of the design, implementation, monitoring and evaluation of policies and programmes in all political, economic and societal spheres, so that inequality is not perpetuated. Moreover, the gender perspective must necessarily be intersectional to be effective. This implies considering the interaction of gender with the multiple elements of our identities – such as social class, race,

ethnicity, sexual orientation and gender expression, among others – to produce patterns of exclusion.

Strong cybersecurity strategies that put people and gender at the centre of public policies and actions are an important response to TFGBV and an important alternative to the use of cybercrime norms.

Civil society participation in the discussion of cybercrime laws and norms is crucial, as well as ensuring meaningful participation that guarantees the inclusion of different expertises and representation for women and other marginalised groups. Civil society organisations provide not only their unique expertise on human rights in general and digital rights in particular, but also bring key and updated information on many technical issues related to the digital environment.

HOW APC WORKS ON THIS ISSUE

APC develops research and analysis on this issue. In 2008, APC launched a dedicated edition of GenderIT focusing on the issue of cybercrime legislation through a gendered perspective. This publication sought to respond to concerns raised by our network on the increasing pervasiveness of cybercrime laws in different regions and their potential impact on women's rights.

A 2010 interview published by APC's Policy Monitor in Latin America and the Caribbean (LAC) indicated that in the region, cybercrime bills were being used to restrict the exercise of women's rights, directly or indirectly. Under the justification of addressing alleged criminal behaviour, these bills considered it necessary to restrict individual rights – specifically, the right to privacy – through discretionary mechanisms to intercept communications or investigate people's private lives without a court order. Other laws entered into conflict with certain constitutional guarantees, such as the right to due legal process, in relation to the use of undercover agents, for example. Both of these situations could be related to restrictions on the exercise of gender rights.

In 2017, APC launched Unshackling Expression: A study on laws criminalising expression online in Asia. The report pointed out how freedom of expression and opinion online is increasingly criminalised with the aid of penal and internet-specific legislation. The original report brought together analysis on the criminalisation of online expression from six Asian states: Cambodia, India,

Malaysia, Myanmar, Pakistan and Thailand. Later editions covered the Philippines, Indonesia and Nepal.

In 2023, teaming up with our Chilean member organisation Derechos Digitales, APC revisited this topic and developed new research on how national cybercrime laws have been used to silence and criminalise women and LGBTQIA+ people around the world. Based on an analysis of legal frameworks adopted in various countries, the study identified 11 cases in Cuba, Egypt, Jordan, Libya, Nicaragua, Russia, Saudi Arabia, Uganda and Venezuela.

Moreover, APC follows and engages directly in policy discussions on this topic at global, regional and national levels. With Derechos Digitales, APC contributed to the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. This submission highlighted concerns about the abusive use of national cybercrime legislation as a tool to undermine human rights, and stressed the importance of ensuring that every normative proposal is consistent with the obligations assumed by member states in international human rights law.

WHERE IS THE DISCUSSION TAKING PLACE?

The UN General Assembly, through its Resolution 74/247, established an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. The Ad Hoc Committee to Elaborate a Comprehensive International Convention approved a roadmap and mode of work for the Committee at its first session, held from 28 February to 11 March 2022. The UN has a specific website with information on multistakeholder participation in the sessions of the Ad Hoc Committee. Various organisations – such as APC and Derechos Digitales, Chatham House and the Electronic Frontier Foundation (EFF) – have contributed commentaries on draft versions of the Convention, particularly about its impact on women and other historically excluded groups. In a joint statement, more than 100 civil society organisations and independent experts stated that the latest draft of the Convention lacks effective gender mainstreaming, which is critical to ensure that the treaty is not used to undermine people's human rights on the basis of gender.

SOME SPACES TO ENGAGE WITH

UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

SOME ORGANISATIONS WORKING ON THIS ISSUE

- Chatham House
- Derechos Digitales
- Electronic Frontier Foundation (EFF)
- Foundation for Media Alternatives (FMA)
- Global Partners Digital (GPD)
- Human Rights Watch
- Red en Defensa de los Derechos Digita les (R3D)

READ MORE

When protection becomes an excuse for criminalisation: Gender considerations on cybercrime frameworks (APC and Derechos Digitales)

Joint statement on the proposed cybercrime treaty ahead of the concluding session (APC and others)

Contribution to the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Derechos Digitales and APC)

Unshackling Expression: A study on laws criminalising expression online in Asia (APC)

Unshackling Expression: A study on online freedom of expression in Indonesia (Alghiffari Aqsa, APC and the Cyrilla Collaborative)

Unshackling Expression: A study on criminalisation of freedom of expression online in Nepal (Body & Data and APC)

Unshackling Expression: The Philippines Report (Foundation for Media Alternatives, APC and the Cyrilla Collaborative)

Cybercrime legislation and gender (GenderIT.org)

Integrating gender in cybercrime capacity-building (Chatham House)

Gender mainstreaming and the proposed cybercrime convention: Commentary on the consolidated draft (Chatham House)