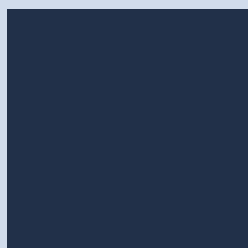
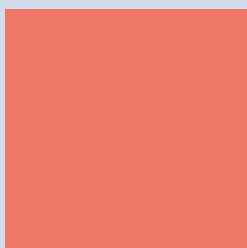
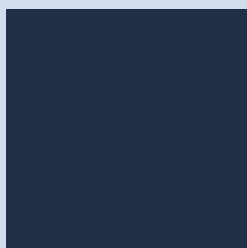
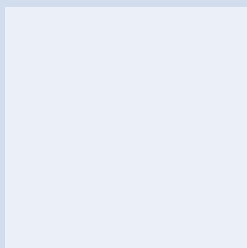
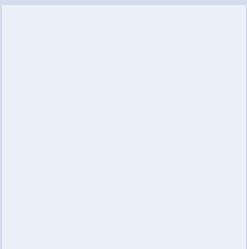
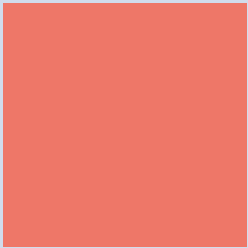
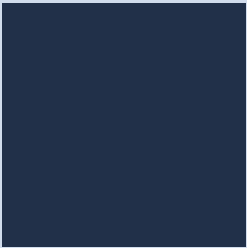
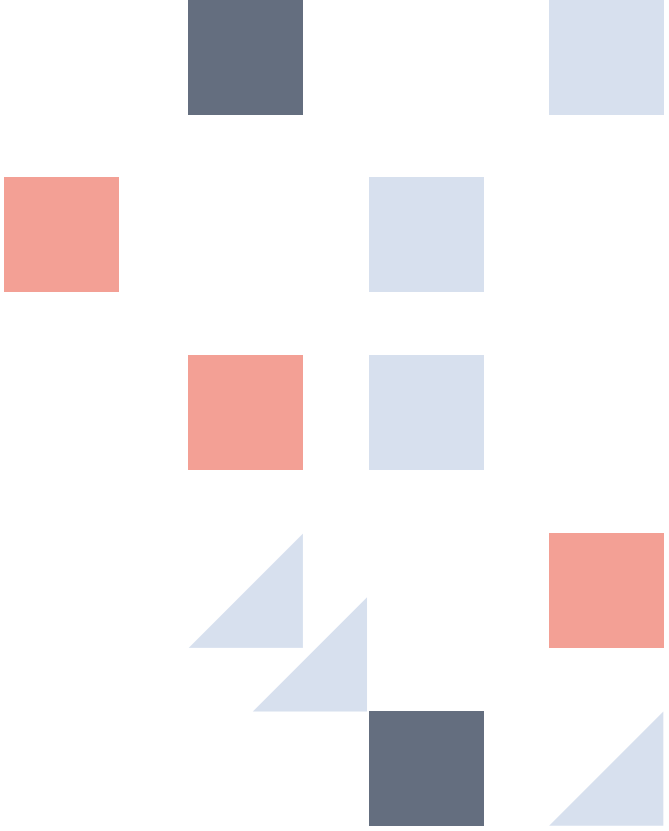


Fostering inclusive cyber norms: a Fundación Karisma case study






In July, GPD published the Inclusive Cyber Norms Toolkit, a pathbreaking new resource which aims to support and empower policymakers and other stakeholders to ensure a fully inclusive approach to the development and implementation of cyber norms.

To help situate and make vivid the key lessons and principles set out by the Toolkit, we commissioned three civil society organisations working in Latin America: Derechos Digitales (Chile), R3D (Mexico) and Fundación Karisma (Colombia) to write case studies, describing their experiences advocating around cybersecurity and human rights.

Below, we present the third case study, by Karisma.

Background and context



In September 2022, Karisma was asked by the technical secretariat of the Netherlands Institute for Multiparty Democracy to be part of the Observatorio de Violencia Contra las Mujeres en Política (Observatory of Violence Against Women in Politics) to build indicators of violence against women in politics. The **Observatory** is a “network of international cooperation and state actors working on the monitoring and analysis of violence against women in politics in Colombia”. It links with the recommendation of the **UN Committee on the Elimination of Discrimination Against Women (CEDAW)**, of the **Committee on the Status of Women (CSW)** and of the Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women on how to address violence against women in politics online.

What was your organisation's aim in getting involved in this process?

Our aim was to bring to the Observatory our experience and **research** on what happened to women candidates during the 2022 congressional elections in Colombia, and the different forms of violence candidates faced, including situations that compromised their security. It was also to argue that legal responses to the problem of violence should not affect rights such as freedom of expression and privacy, like we have **done** in the **past**.

Building from that expertise, our main purpose was to ensure that evidence of those situations could help shape future regulatory proposals, and to contribute a human rights perspective on the regulation of the digital environment.

What challenges did you anticipate when you were entering the process? How did your organisation prepare for these challenges?

Initially, we joined the Observatory to develop indicators related to violence against women politicians, since the main function of the observatory was to gather qualitative and quantitative information for a biannual report on the situation of violence faced by women politicians. However, in 2022, a bill was presented to Congress on violence

against women in politics which aimed at implementing the OAS **Inter-American model law on the Prevention, Punishment, and Eradication of Violence against Women in Political Life**. As a result, we began to engage in the bill process, which quickly took over the work of the Observatory. This unexpected change of scope was the first challenge. However, our clear interest and value-add in participating in the process—providing our experiences and supporting civil society groups to ensure digital rights considerations were incorporated into the bill—meant we were able to adjust our focus as priorities changed.

Discussions relating to the Observatory and to the bill were complex. Through the Observatory, Karisma and other stakeholders created a parallel text for the draft bill, intended to inform the ongoing negotiations. The process of developing this parallel text was challenging, as stakeholders participating in this Observatory had diverse aims and perspectives. Not all of the proposals from the Observatory were fully supported by all stakeholders. Karisma withdrew its support from certain proposals which undermined human rights and particularly freedom of expression (for instance, by blocking content or suspending the accounts of users as means of promoting safe online spaces).

At the same time, the draft text included a number of guarantees for human rights and it was our priority to ensure these were maintained as the bill passed through Congress. The democratic debate in the Congress meant that the number of actors engaging in discussions and the diversity of their perspectives and interests also increased. We knew that any agreements reached by consensus through the Observatory discussions were more likely to successfully make it through Congress, whereas dissenting positions would need to be defended with members of the Congress one by one. The follow up and intensive advocacy required at the legislative stage is a demanding activity for civil society.

What happened?



In Observatory discussions, Karisma contributed to the definition of differential risks for women in politics, including cybersecurity—helping to fill a knowledge gap at the Observatory, which generally lacks members with expertise in technology.

The Observatory provided a space for multistakeholder dialogue on policy solutions to address violence against women in politics and its online dimensions. The work done through the Observatory helped different stakeholders to understand the role and responsibility of the state, and demonstrated the important role played by civil society (local and international) in developing and implementing policy solutions, including as they relate to cybersecurity risks and the protection of human rights.

However, the eagerness to achieve the approval of the bill—which had to be passed within a single legislature—limited space for consultation and dialogue. Although we

presented our criticisms early in the process, the tension between the exercise of the right to live a life free of violence and other rights, such as freedom of expression and privacy, proved difficult to overcome. Attempts to explain the implications of certain proposals on technical processes—relating to the internet, social networking platforms, and state powers over internet traffic—were not fully fruitful.

In the end, it was not possible to reach consensus on the need for women-centred remedies, including prevention, care and redress. Nor was it possible to secure an exemption for journalistic and citizen oversight work from gender based violence sanctions. On the contrary, quite broad definitions of what constitutes violence were included, and an administrative authority was given the power to decide what content on social networks counts as disinformation and to impose sanctions accordingly. The possibility of eliminating digital propaganda that affects women, without establishing due process, was also raised.

At the time of writing, the process is still ongoing, and is scheduled to end in 2024. As the draft law aims to become a statutory law, it will have to be approved both in Congress and by the Constitutional Court.

We continue to scrutinise the draft law and to raise awareness of potential challenges it presents to the exercise of human rights online.

Did policymakers work to make the process inclusive?

Unusually for regulation in Colombia, this process has been relatively people-centred in that it has focused on a specific impacted group (women in politics). The organisations that are part of the Observatory are familiar with the struggles of female politicians. However, it would have been desirable to have a more open process, with representatives from different regions of the country. While the Observatory's work is not about cybersecurity explicitly, the government has indicated that their longer term goal is to approach cybersecurity in a similarly people-centred manner.

During the process, the Observatory has made efforts to reach out to women affected by violence in political life. This has enabled a more holistic debate within the process on human impacts.

Recommendations

For civil society

- *Ensure that you have resources and capacity to participate during the entirety of the process.*
- *Find non-obvious routes to engage policymakers on cybersecurity.* In this case, the broader framing of violence against women gave us an opportunity to talk about cybersecurity considerations and the way they affect these groups.
- *Prepare the ground with examples and clear messages.* This will facilitate greater understanding of more technical issues (i.e. cybersecurity risks), particularly in the context of a complex debate that includes very diverse actors.
- *Build joint positions with other NGOs that participate in the process* (in this case, the Observatory). However, this can be challenging when organisations have different values or positions on human rights.
- *Establish agreement as soon as possible within the process on how to express dissent constructively.*
- *Agree your NGO's position before meetings.*

For policymakers

- *Consult and solicit comments from different stakeholders*, especially those from the most affected groups.
- *Ensure that opportunities for participation reflect the diverse experiences, needs and perspectives of different stakeholders.*
- *Proactively seek input from the most affected groups* and seek to understand, balance and respect different approaches, including contradictory ones.
- *Ensure that there are coordination mechanisms and educational measures in place to help achieve public buy-in and understanding of key provisions*, whose significance and impacts can be hard to understand. Although, historically, Colombian policymakers have regulated cybersecurity issues from a criminal law perspective, thinking about regulation in terms of the promotion of education about cybersecurity and digital rights could be a way to empower citizens.