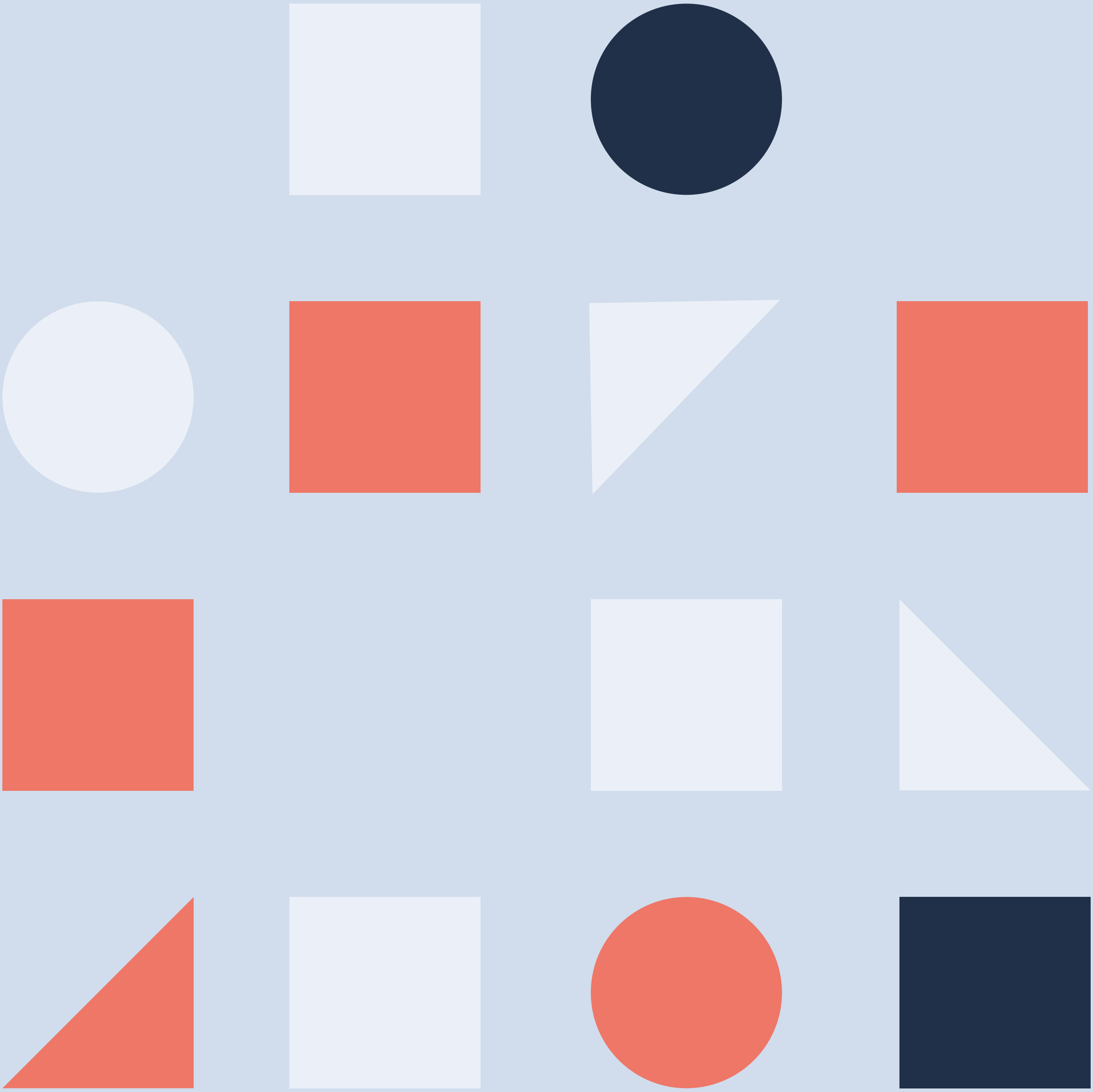
Fostering inclusive cyber norms: an R3D case study



GLOBAL PARTNERS DIGITAL

2023

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 second case study, by R3D.

Background and context

There is currently no specific federal cybersecurity law in force in Mexico. However, in recent years, discussions have emerged around whether Mexico should sign the Budapest Convention on Cybercrime, and on the need to address consistent threats to the country's critical infrastructure. As a result of these discussions, a national cybersecurity bill was introduced into the Mexican National Congress in 2023.

At the time of writing, the bill is awaiting opinions from the relevant commissions; therefore the legislative process remains pending.

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

In various forums, R3D has consistently advocated for a human-centric approach to cyber norms and cybersecurity. This includes supporting the need for an evidence-based approach to cybersecurity governance, which includes all relevant stakeholders.

In the case of the national cybersecurity bill in Mexico, it was clear to us that the stakes for human rights were high. On the one hand, a cybersecurity law could have positive impacts at the national level—aiding the implementation within Mexican institutions of the normative framework of responsible state behaviour in cyberspace in a rights-respecting and human-centric manner (for example, by ensuring protection for security researchers). Conversely, it could also undermine human rights (for example, by legitimising the use of surveillance without adequate safeguards).

In engaging with the development of the bill, our key goal was ensuring that basic protections for privacy and freedom of speech were included: specifically, avoiding any procedural measures for criminal investigations without proper precautions. We also aimed to ensure that the bill emphasised the protection and security of people (a human-centric approach).

At what stages did your organisation engage? And in what ways?

In January 2020, before the national cybersecurity bill was presented, R3D participated in various government-led panel discussions and capacity-building workshops on cybersecurity, which took a multidisciplinary and multistakeholder approach. At these sessions, we set out ten human rights principles for cybersecurity legislation.

However, in July 2022, we became aware that the Senate and the Chamber of Representatives' Science and Technology Committees were organising separate consultations around a proposed new national cybersecurity draft law. These consultations did not seek civil society engagement, leaving us with limited opportunities to contribute our perspectives and insights.

Unlike prior attempts to make cybersecurity legislation in Mexico, this bill had joint support from different parties across the political spectrum and was primarily sponsored by the current administration. In our assessment, this made it more likely to pass, and therefore more potentially concerning from a human rights perspective, which added urgency to our engagement.

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

There were two main challenges to engaging with this process:

- The consultations in 2022 were not inclusive. They consulted only with other government offices and sought business sector input; they did not reach out to gather civil society perspectives.

- The army—represented by the defence and marine secretaries—were the leading proponents of the law. This meant that the process was 'owned' by agencies whose decision-making processes are opaque, and where there is very little to no opportunity for multistakeholder participation. Previous efforts by some civil society organisations, including our own, have also made these agencies wary of engaging with civil society. For example, in 2022, R3D presented an investigation that exposed the army's illegal surveillance of human rights defenders, journalists, and political opponents.

What happened

In August 2022, we reached out to one of the chairs of the Commissions in charge of drafting the new cybersecurity bill. The aim of this outreach was to explain and emphasise the need for an open process in which human rights organisations could fully participate, and the need to adopt a human rights approach in any cybersecurity legislation.

The Commissions' teams were accessible at first, and agreed that it was better to have input from civil society with experience on cyber norm implementation and human rights in the early stages, rather than pass an unconstitutional law which could later be struck down by the courts. However, no follow up was received and so, in practice, the process continued without input from non-governmental stakeholders.

We delivered statements and interviews to the media to push for the inclusion of human rights organisations, researchers, and other relevant stakeholders. This had an impact: delaying the presentation of a rushed zero draft of the bill that could be approved in the shadows. In response to this growing pressure, the Commissions in charge of drafting the law organised an "open parliament" exercise in October 2022. However, very limited notice was provided, the event took place solely online, and speakers were only allowed two minutes each. This meant that it was not possible for civil society and academia to engage meaningfully.

Nevertheless, this limited opportunity still provided us with welcome exposure to the process. Two lawmakers approached us after we delivered our short but concise and coordinated statements at the open parliament, proposing that we organise a panel and a workshop with lawmakers and relevant stakeholders to foster a better understanding of the implications of the proposed national cybersecurity law. These panel discussions took place in May 2023 at the House of Representatives, where we raised awareness about the need for cyber norms based in a human rights perspective.

Did policymakers work to make the process inclusive?

While we have increased awareness regarding the impact of cyber norms on gender and marginalised groups, policymakers have yet to take substantive steps to incorporate this and meaningfully engage with these groups.

Initial efforts were made to include diverse groups, but the absence of follow-up and transparency in the policymaking process resulted in a lack of meaningful engagement and genuine inclusion. This highlights that an inclusive and transparent process at every stage of policymaking is essential to ensure effective engagement with these groups, as well as the active involvement of relevant stakeholders to foster a common understanding of the impact of these policies on the most vulnerable groups.

Recommendations

For civil society

- *Early engagement is crucial.* By actively participating in consultations relating to the national cybersecurity bill in the early stages, we helped lawmakers to recognise the importance of civil society inclusion. This early engagement facilitated our later involvement in initiatives such as the open parliament and the organisation of human rights-based panel discussions at the House of Representatives.

- *Be flexible.* Even though opportunities for stakeholders were limited, we continued our engagement alongside a coalition of local civil society groups participating in other cyber events. Key decision makers also participated in these events and attended conferences, giving us the opportunity to talk to them and make our points heard in other ways.

- *Constantly monitor discussions.* Timing is crucial for advocacy. We are constantly monitoring the agendas for the Senate and Chamber of Representatives for updates. This helps us to map whether there are new bills or relevant events and to act accordingly.

- *Coordinate an alliance with other relevant organisations and stakeholders.* Legislators are often more willing to listen to civil society if they are in a collective of multiple organisations. Relevant lawmakers and stakeholders heard our requests for an open process because it was a consistent message across statements from several human rights organisations.

- *Make statements and engage with the press.* We were able to increase the political cost of blocking civil society engagement by building pressure through the media. We contacted journalists covering tech to tell them about the dangerous consequences a national cybersecurity law sponsored by the military could have on human rights.

- *Have a strategy document with goals ranging from low-hanging fruit to the best outcome possible.* We had a bad opening hand in the negotiations so we needed to be flexible and strategic. We created a document with our principal non-negotiable goals: like having essential safeguards around criminal investigations, and avoiding the incorporation of crimes that would criminalise conduct permitted under international human rights law.

- *Leverage international forums:* Having an international presence in cybersecurity forums helped us gain more allies in different areas. For example, the Mexican secretary of Foreign Affairs is participating in the drafting process of the cybersecurity bill, as well as in international cyber discussions. This provided us with the opportunity to sustain momentum on discussions, share timely updates, and follow up with relevant actors.

For policymakers

- ***Initiate early engagement with civil society***. Incorporate groups beyond government and the private sector into the process.
- ***Seek strategic and inclusive alliances for more meaningful advocacy***. Include organisations specialised in digital rights and organisations with different relevant focuses to ensure inclusion, such as children's rights and gender-based rights.
- ***Create flexible and meaningful ways for stakeholders to engage***. Provide timely information, establish clear lines of communication and reporting, allow enough time for interventions, and allow contributions in all formats (written, oral, audiovisual, etc).
- ***Engage relevant stakeholders in reflection and analysis dialogues throughout the policy process.***
- ***Record lessons and experiences learned throughout the process to ensure accountability and transparency***. This documentation might include details of substantive policy differences and instances where commitments to inclusive participation were not met. It could also document instances where stakeholders within the process were marginalised or discriminated against: e.g. through having their views sidelined, or the authenticity or value of their input questioned. ***Seize the opportunity presented by national policy-making processes to operationalise commitments at the global level***: align national cyber policymaking processes with their commitments to implement the internationally agreed norms of responsible state behaviour in cyberspace.
- ***Proactively implement stakeholder perspectives to foster substantive and meaningful engagement.***