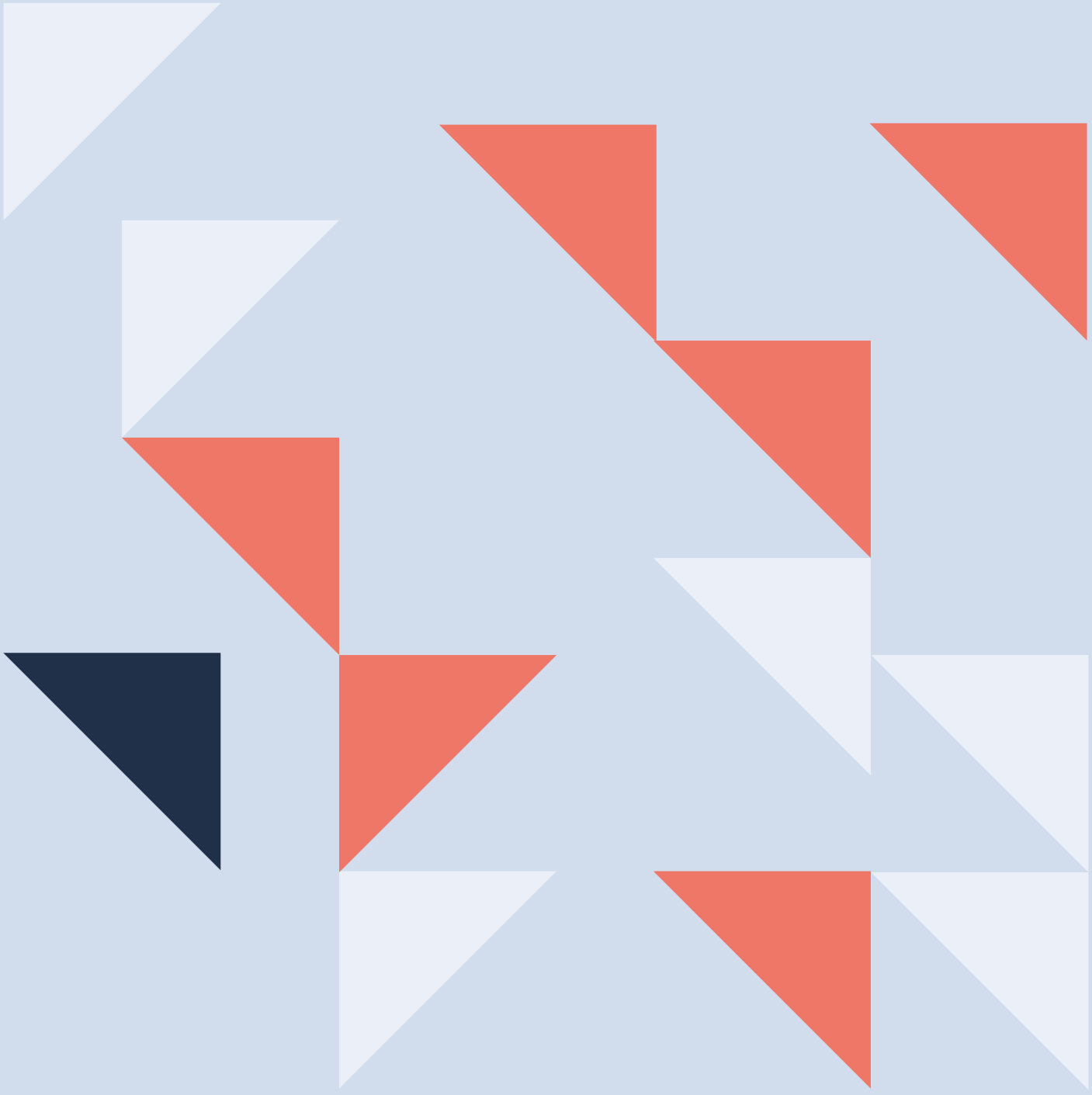
Fostering inclusive cyber norms: a Derechos Digitales case study



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 (Latin America), R3D (Mexico) and Fundación Karisma (Colombia) to write case studies, describing their experiences advocating around cybersecurity and human rights.

Below, we present the first case study, by Derechos Digitales, on Chile.

Background and context

In 2017, a new National Cybersecurity Policy 2017-2022 (PNCS) was developed in Chile by the government of President Bachelet, setting guidelines for the State of Chile to safeguard the security of people and their rights in cyberspace. In 2018, President Piñera reaffirmed the PNCS as a state policy, advancing its implementation, including the introduction of the draft Framework Law on Cybersecurity and Critical Infrastructure the same year as one of the measures of the Policy. The PNCS provided a roadmap to advance the implementation of the internationally agreed upon norms to ensure a safe cyberspace for all, including responsible state behaviour and the protection of infrastructure.

In August 2022, the government announced the development of a new national policy (2023-28) to replace the PNCS. It was billed as a way of providing more concrete measures to addressthreats and vulnerabilities, while creating a new institution dedicated specifically to cybersecurity management in the country.

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

In the process to develop the 2017-2022 PNCS, there was a remarkable level of openness, transparency and inclusive participation, including by Derechos Digitales. When it was time for a new national policy, it was expected that there would not only be similar participation but further inclusiveness. However, after 2022 no new draft policy was in place to replace the 2017-2022 PNCS or continue the work. Although the draft Framework Law was moving forward in Congress, it wasn't until mid-2022 that the new national policy was announced, alongside an evaluation of the success of the previous policy (the 2017-2022 PNCS).

Amid this lack of information, concerns about the new national policy development process were raised by Derechos Digitales and other groups: How would international cyber norms be implemented substantively? How different would participation be in comparison to the previous process, and how would gender and human rights considerations be advanced in the new draft? These were the core priorities we had going into the process.

What happened (so far)

Organisations from civil society, academia, the technical community and the private sector were invited to public hearings with the Inter Ministerial Committee in early 2023, with the purpose of providing inputs for the drafting of the national policy 2023-2028, to contribute constructively and critically to the process by discussing a working document which laid out the basis of the new policy. We learnt during that period that there was an ongoing evaluation of the first process, and that the national policy for 2023-2028 would be drafted in parallel to that assessment.

The process continued without much fanfare, while also making room for public participation. The first Citizens' Consultation on Cybersecurity 2023 was launched in March and a second one in May, allowing access to a first version of the proposed new policy. These consultations focused on individual capacities and understanding of topics rather than being based on stakeholder group or institutional affiliation. These consultations were presented as online surveys, and the aforementioned lack of fanfare meant that there would not be large awareness efforts. In that regard, the process would still be limited to those privy to its existence.

The effort to engage women and girls more explicitly was limited to the first public consultation. The results, published in April, were accordingly skewed towards men from more privileged backgrounds. Only 37.2% of respondents identified as female. Though a valuable effort, it seems like this process did not reach enough people or communities to effectively engage them, which could affect the result of the issues perceived as less important, such as gender approach and parity. We also did not observe any analysis regarding the gender approach or the inclusion of children and adolescents, and the findings did not reflect on marginalised groups. A similar analysis of the second public consultation was not made public.

The public at large finally knew about the new draft policy when it was publicly finalised, in an announcement made by the President in late May 2023. The new national policy would thus follow five core objectives in line with the previous one: fostering a resilient infrastructure, rights online, a culture of cybersecurity, national and international coordination, and cybersecurity industry and research. The announcement was not accompanied by a public version of the finalised policy or by the assessment of the previous policy (the 2017-2022 PNCS). After the announcement, much of the emphasis by the government was placed on the discussion of the draft Framework Law.

Though we acknowledge the steps taken to maintain public participation through public hearings, public consultations, and an emphasis on gender considerations, there was limited engagement in general and a lack of clarity on the stages and timelines of the whole process. The new policy is expected to be launched by the fourth quarter of 2023.

Recommendations

For civil society

- ***Maintaining relationships of trust is essential.*** The ability to gain insider knowledge about ongoing processes often requires existing links with involved personnel, including those present in previous iterations of policy processes. By maintaining good communications and relying on our own openness in candid conversations, we were able to intervene in the process and gain relevant information.

- ***Make high expectations known.*** Since long policy processes may have fewer instances of participation and inclusiveness, expectations must be known to the authorities and the public, in order to encourage change and help steer processes towards desired outcomes.

- ***Engage other stakeholders.*** Knowing different stakeholders and engaging with them can be useful for gaining insight on common concerns and further insights in policy processes. This requires devoting time and resources and casting a wide net to identify and reach affected communities that might not initially appear as obvious stakeholders in cyber policy. It is also important that these efforts allow different stakeholders to engage with each other and create synergies among stakeholder groups.

For policymakers

- ***Make processes widely known***, setting clear timelines and instances for public participation. In the case of Chile, this happened to a limited extent and the launch and publication of certain documents was not as well-publicised as expected.

- ***Ensure inclusion and use accessible language*** when engaging with different stakeholders with different levels of expertise, especially those that may be coming to the subject for the first time.

- ***Model transparency by publishing stakeholder inputs***. Although there was a strong focus on inclusivity in the public consultations for this process, the publication of the received stakeholder inputs would have been useful to know whether there was sufficient outreach to different communities. In the case of open public consultations, if they refer to specific individuals and groups in situations of vulnerability, statistics and findings should ensure anonymity for respondents.

- ***Engage early, widely and often***. Though seemingly highly technical in nature, cyber policy and cyber norm implementation processes need to include all impacted stakeholders, and not just representatives from more engaged institutions.