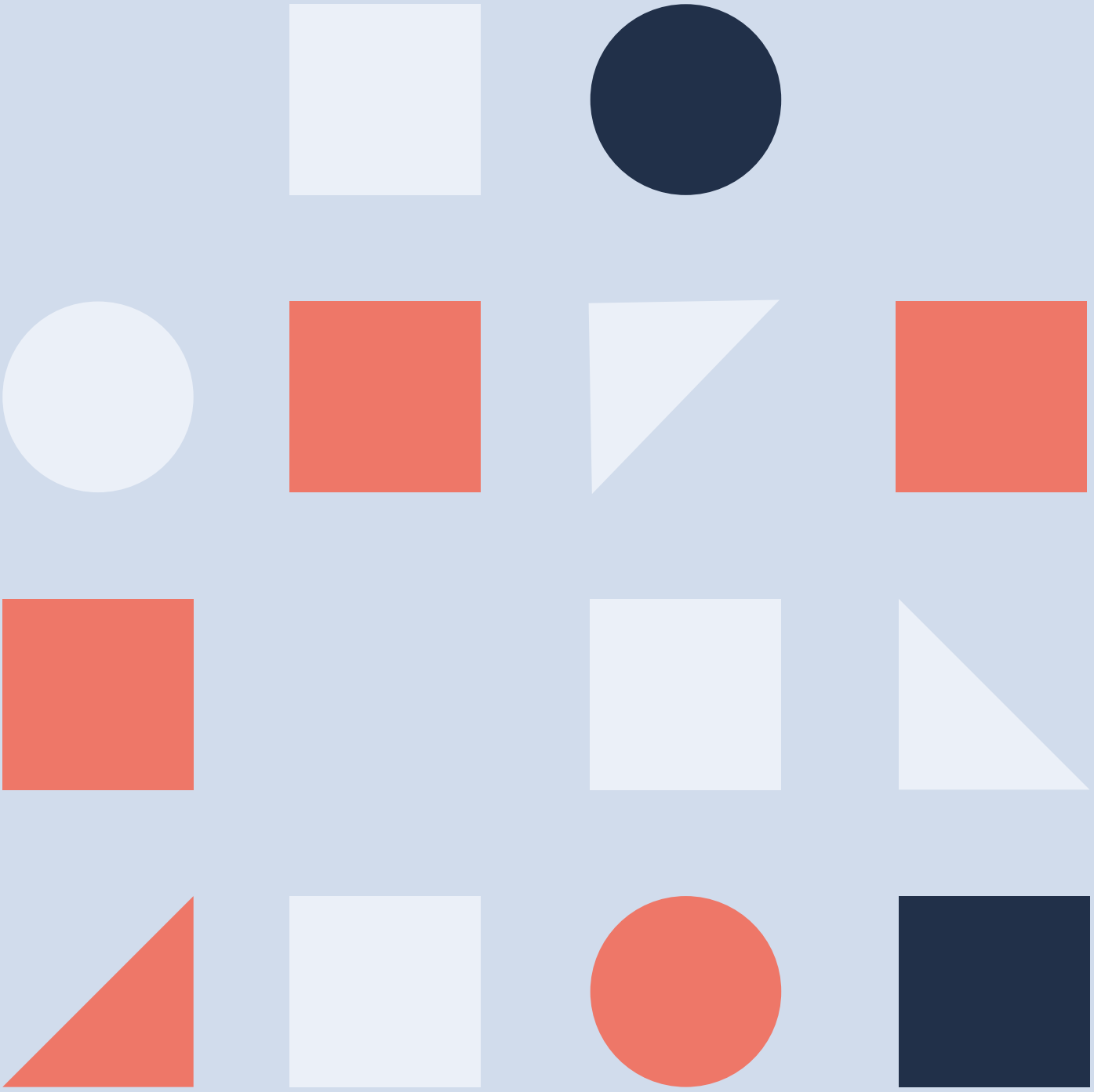
Promoción de cibernormas inclusivas: un estudio de caso de R3D



GLOBAL PARTNERS DIGITAL

2023

En julio, GPD publicó la Guía para Cibernormas Inclusivas, un nuevo recurso pionero cuyo objetivo es apoyar y capacitar a personas que se encargan de la formulación de políticas y a otras partes interesadas para garantizar un enfoque plenamente inclusivo en el desarrollo e implementación de cibernormas.

Para ubicar y dar vida a las lecciones y principios clave establecidos en la Guía, se encargó a tres organizaciones de la sociedad civil que trabajan en América Latina (Derechos Digitales (América Latina), R3D (México) y Fundación Karisma (Colombia) que escribieran estudios de caso, en los que describieran sus experiencias de defensa de la ciberseguridad y los derechos humanos.

A continuación se presenta el segundo estudio de caso, realizado por R3D.

Antecedentes y contexto

En la actualidad no existe una ley federal específica de ciberseguridad vigente en México. Sin embargo, en los últimos años, han surgido debates en torno a si México debe suscribir el Convenio de Budapest sobre la Ciberdelincuencia, y sobre la necesidad de hacer frente a las amenazas significativas a las infraestructuras críticas del país. Como resultado de estas conversaciones, en 2023, se introdujo un proyecto de ley nacional de ciberseguridad en el Congreso Nacional de México.

En el momento de redactar este informe, el proyecto de ley está a la espera de los dictámenes de las comisiones competentes, por lo que el proceso legislativo sigue abierto.

¿Qué objetivo tenía su organización al involucrarse en este proceso?

En diversos foros, R3D ha abogado sistemáticamente por la adopción de un enfoque de cibernormas y ciberseguridad centrado en el ser humano. Esto incluye apoyar un enfoque de gobernanza de la ciberseguridad que esté necesariamente basado en evidencia e incluya a todas las partes interesadas.

En el caso del proyecto de ley nacional de ciberseguridad en México, nos quedó claro que era mucho lo que estaba en juego para los derechos humanos. Por un lado, una ley de ciberseguridad podría tener efectos positivos a nivel nacional, ya que ayudaría a implementar en las instituciones mexicanas el marco normativo de un comportamiento estatal responsable en el ciberespacio, respetuoso con los derechos y centrado en las personas (por ejemplo, garantizando la protección de los investigadores de seguridad). Por el contrario, también podría socavar los derechos humanos (por ejemplo, al legitimar el uso de la vigilancia sin las garantías adecuadas).

Al participar en la elaboración del proyecto de ley, nuestro principal objetivo era garantizar que se incluyeran protecciones básicas para la privacidad y la libertad de expresión: en concreto, evitar que se tomen medidas procesales en el marco de las investigaciones penales sin las debidas precauciones. También nos propusimos garantizar que el proyecto de ley hiciera hincapié en la protección y la seguridad de las personas (un enfoque centrado en el ser humano).

¿En qué fases participó su organización? ¿Y de qué manera?

En enero de 2020, antes de que se presentara el proyecto de ley nacional de ciberseguridad, R3D participó en varias mesas redondas y talleres de capacitación sobre ciberseguridad dirigidos por el Gobierno, en los que se adoptó un enfoque multidisciplinario y de múltiples partes interesadas. En estas sesiones, establecimos diez principios sobre ciberseguridad y derechos humanos.

No obstante, en julio de 2022, supimos que las Comisiones de Ciencia y Tecnología del Senado y de la Cámara de Representantes estaban organizando consultas separadas en torno a un nuevo proyecto de ley nacional sobre ciberseguridad. Estas consultas no contemplaban la participación de la sociedad civil, lo que nos dejaba pocas oportunidades de aportar nuestras perspectivas y puntos de vista.

A diferencia de intentos anteriores de legislar en materia de ciberseguridad en México, este proyecto de ley contó con el apoyo conjunto de diferentes partidos de todo el espectro político y fue patrocinado principalmente por la administración actual. A nuestro juicio, esto hacía que fuera más probable que se aprobara y, por lo tanto, más preocupante desde la perspectiva de los derechos humanos, lo que acentuaba la importancia de nuestra participación.

¿Qué dificultades anticipaban al iniciar el proceso? ¿Cómo se preparó la organización para afrontarlas?

Participar en este proceso planteaba dos retos principales:

- Las consultas de 2022 no fueron inclusivas. Solo se consultó a otras administraciones públicas y se recabó la opinión del sector privado; no se trató de recoger las perspectivas de la sociedad civil.

- El ejército —representado por los secretarios de Defensa y Marina— fue el principal defensor de la ley. Esto significa que el proceso fue «propiedad» de organismos cuyos procesos de toma de decisiones son opacos, y en los que hay muy pocas o ninguna oportunidad para la participación de múltiples partes interesadas. Los esfuerzos anteriores de algunas organizaciones de la sociedad civil, incluida la nuestra, también han hecho que estas agencias se muestren reacias a colaborar con la sociedad civil. Por ejemplo, en 2022, R3D presentó una investigación que sacaba a la luz la vigilancia ilegal del ejército sobre personas defensoras de los derechos humanos, periodistas y opositoras políticas.

¿Qué sucedió?

En agosto de 2022, nos pusimos en contacto con la persona que presidía una de las comisiones encargadas de redactar el nuevo proyecto de ley sobre ciberseguridad. El objetivo de este contacto era explicar y destacar la necesidad de que hubiera un proceso abierto en el que pudieran participar plenamente las organizaciones de derechos humanos, así como la importancia de adoptar un enfoque de derechos humanos en toda legislación sobre ciberseguridad.

Los equipos de las Comisiones se mostraron accesibles en un primer momento, y coincidieron en que era mejor contar con aportes de la sociedad civil con experiencia en la implementación de cibernormas y derechos humanos en las primeras fases, en lugar de aprobar una ley inconstitucional que posteriormente pudiera ser anulada por los tribunales. Sin embargo, no se recibió ninguna respuesta, por lo que, en la práctica, el proceso continuó sin aportes de las partes interesadas no gubernamentales.

Hicimos declaraciones y entrevistas en los medios de comunicación para presionar por que se incluyera a organizaciones de derechos humanos, investigadores y otras partes interesadas. Esto surtió efecto: se retrasó la presentación de un precipitado anteproyecto de ley que podría aprobarse en la sombra. En respuesta a esta creciente presión, las comisiones encargadas de redactar la ley organizaron un ejercicio de «parlamento abierto» en octubre de 2022. Sin embargo, se avisó con muy poca antelación, el acto se celebró únicamente por Internet y solo se concedieron dos minutos a cada persona que intervenía. Esto impidió que la sociedad civil y el mundo académico participaran de forma significativa.

No obstante, esta oportunidad, si bien limitada, nos permitió conocer el proceso. Dos responsables de la elaboración de leyes se pusieron en contacto con nuestra organización tras nuestras breves pero concisas y coordinadas declaraciones en el parlamento abierto, y nos propusieron organizar una mesa redonda y un taller con más representantes y partes interesadas para fomentar una mejor comprensión de las implicaciones de la propuesta de ley nacional de ciberseguridad. Estas mesas redondas tuvieron lugar en mayo de 2023 en la Cámara de Representantes, donde concientizamos sobre la necesidad de cibernormas basadas en una perspectiva de derechos humanos.

¿Las personas encargadas de la formulación de políticas velaron por que el proceso fuera integrador?

Si bien se ha incrementado la concientización sobre el impacto de las cibernormas en los grupos marginados y de género, las autoridades responsables de la formulación de políticas aún no han tomado medidas de fondo para incorporarlo y comprometerse de forma significativa con estos grupos.

Se hicieron esfuerzos en un primer momento para incluir a diversos grupos, pero la ausencia de seguimiento y transparencia en el proceso de elaboración de las políticas se tradujo en una falta de compromiso efectivo y de verdadera inclusión. Esto pone de relieve la importancia de que el proceso de elaboración de las políticas sea inclusivo y transparente en todas sus fases para garantizar una participación efectiva de estos grupos, así como la implicación activa de las partes interesadas pertinentes para fomentar un entendimiento común del impacto de estas políticas en los grupos más vulnerables.

Recomendaciones:

Para la sociedad civil

- ***La participación temprana es crucial.*** Al participar activamente en las consultas relacionadas con el proyecto de ley nacional de ciberseguridad en las primeras fases, ayudamos a las autoridades legislativas a reconocer la importancia de la inclusión de la sociedad civil. Este compromiso temprano facilitó nuestra participación posterior en iniciativas como el parlamento abierto y la organización de mesas redondas sobre derechos humanos en la Cámara de Representantes.

- ***Ser flexibles***. Si bien las oportunidades para las partes interesadas eran limitadas, mantuvimos nuestro involucramiento junto a una coalición de grupos locales de la sociedad civil que participaban en otras instancias sobre ciberseguridad. Las personas clave en la toma de decisiones también participaron en estas instancias y asistieron a conferencias, lo que nos dio la oportunidad de hablar con ellas y hacerles llegar nuestros puntos de vista por otras vías.

- ***Seguir constantemente los debates.*** Los tiempos son cruciales para las actividades de defensa de una causa. Hacemos un seguimiento constante de los órdenes del día del Senado y la Cámara de Representantes para mantenernos al tanto de lo que sucede. Esto nos ayuda a saber si hay nuevos proyectos de ley o acontecimientos relevantes y a actuar en consecuencia.

- ***Coordinar una alianza con otras organizaciones y partes interesadas pertinentes.*** Con frecuencia, las autoridades legislativas están más dispuestas a escuchar a la sociedad civil si forman parte de un colectivo de varias organizaciones. Las autoridades legislativas y las partes interesadas atendieron nuestras peticiones de un proceso abierto porque era un mismo mensaje uniforme en las declaraciones de varias organizaciones de derechos humanos.

- ***Hacer declaraciones y colaborar con la prensa.*** Pudimos aumentar el coste político del bloqueo de la participación de la sociedad civil ejerciendo presión a través de los medios de comunicación. Nos pusimos en contacto con periodistas que cubren el sector tecnológico para informarles de las peligrosas consecuencias que podría tener para los derechos humanos una ley nacional de ciberseguridad patrocinada por el ejército.

- ***Disponer de un documento de estrategia con objetivos que vayan desde lo más fácil de obtener hasta el mejor resultado posible.*** Teníamos una mala mano inicial en las negociaciones, así que tuvimos que valernos de flexibilidad y estrategia. Creamos un documento con nuestros principales objetivos no negociables, por ejemplo, disponer de salvaguardias esenciales en torno a las investigaciones

penales y evitar la tipificación de delitos que criminalizarían conductas permitidas por el derecho internacional de los derechos humanos.

- *Aprovechar los foros internacionales:* Tener presencia internacional en foros de ciberseguridad nos ayudó a generar un mayor número de alianzas en diferentes ámbitos. Por ejemplo, la Secretaría de Relaciones Exteriores de México está participando en el proceso de redacción del proyecto de ley de ciberseguridad, así como en discusiones cibernormas internacionales. Esto nos brindó la oportunidad de mantener el impulso en las discusiones, compartir novedades y dar seguimiento con los agentes relevantes.

Para las instancias responsables de la formulación de políticas

- *Iniciar un diálogo con la sociedad civil en una fase temprana*. Incorporar al proceso a grupos ajenos al gobierno y al sector privado.
- *Buscar alianzas estratégicas e inclusivas para una promoción más significativa*. Incluir organizaciones especializadas en derechos digitales y organizaciones con diferentes enfoques de interés para garantizar la inclusión, como los derechos del niño y los derechos por razón de género.
- *Crear formas flexibles y significativas para involucrar a las partes interesadas*. Facilitar información oportuna, establecer líneas claras de comunicación e información, dejar tiempo suficiente para las intervenciones y permitir contribuciones en todos los formatos (escrito, oral, audiovisual, etc.).
- *Involucrar a las partes interesadas en los diálogos de reflexión y análisis a lo largo de todo el proceso político.*
- *Registrar las lecciones y experiencias aprendidas a lo largo del proceso para garantizar la rendición de cuentas y la transparencia*. Esta documentación puede incluir detalles de las diferencias políticas sustantivas y de los casos en los que no se cumplieron los compromisos de participación inclusiva. También pueden documentarse los casos en los que se marginó o discriminó a las partes interesadas en el proceso, por ejemplo, cuando se dejaron de lado sus opiniones o se cuestionó la autenticidad o el valor de sus aportaciones.
- *Aprovechar la oportunidad que brindan los procesos nacionales de elaboración de políticas para hacer operativos los compromisos a nivel internacional*: alinear los procesos nacionales de elaboración de políticas cibernormas con sus compromisos de aplicar las normas acordadas internacionalmente sobre el comportamiento responsable de los Estados en el ciberespacio.
- *Aplicar de forma proactiva las perspectivas de las partes interesadas para fomentar una participación sustantiva y significativa.*