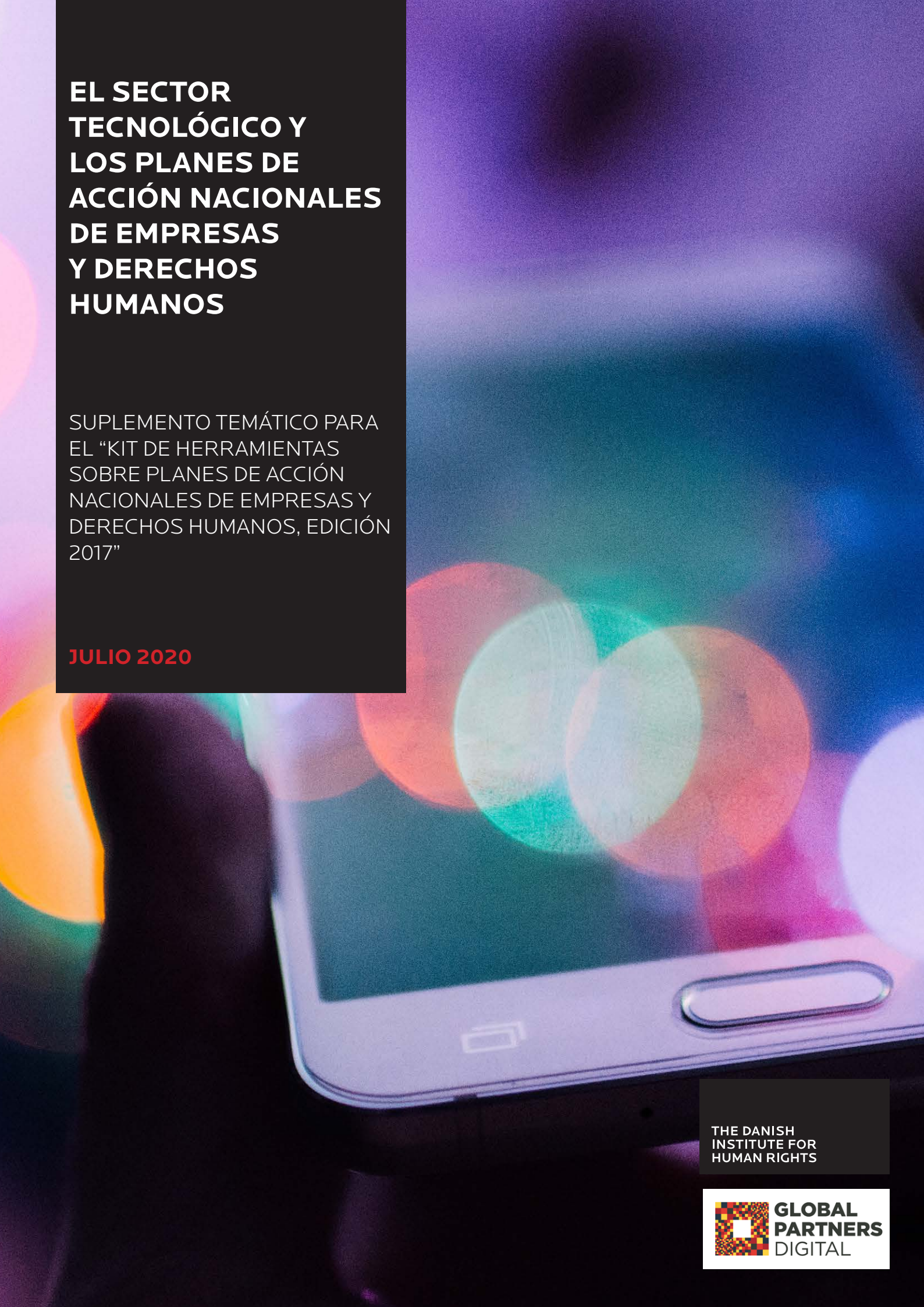
EL SECTOR TECNOLÓGICO Y LOS PLANES DE ACCIÓN NACIONALES DE EMPRESAS Y DERECHOS HUMANOS

SUPLEMENTO TEMÁTICO PARA EL "KIT DE HERRAMIENTAS SOBRE PLANES DE ACCIÓN NACIONALES DE EMPRESAS Y DERECHOS HUMANOS, EDICIÓN 2017"

JULIO 2020



THE DANISH INSTITUTE FOR HUMAN RIGHTS

GLOBAL PARTNERS DIGITAL

EL SECTOR TECNOLÓGICO Y LOS PLANES DE ACCIÓN NACIONALES DE EMPRESAS Y DERECHOS HUMANOS
Suplemento temático para el "Kit de herramientas sobre planes de acción nacionales de empresas y derechos humanos, edición 2017"

THE DANISH INSTITUTE FOR HUMAN RIGHTS

El Instituto Danés de Derechos Humanos (DIHR) es la Institución Nacional de Derechos Humanos de Dinamarca, cuyo mandato es promover y proteger los derechos humanos y la igualdad de trato en Dinamarca y en el extranjero. El Departamento de Derechos Humanos y Empresas es una unidad especializada dentro del DIHR, que centra su atención en el rol que cumple el sector privado en lo que respecta al respeto por los derechos humanos.

GLOBAL PARTNERS DIGITAL

GLOBAL PARTNERS DIGITAL (GPD) es una compañía con fines sociales dedicada a fomentar un entorno digital basado en los derechos humanos y en los valores democráticos. Esto se logra creando procesos y espacios de políticas más abiertos, inclusivos y transparentes, lo que facilita la participación estratégica, informada y coordinada en estos procesos por parte de actores de interés público.

AUTORES

Richard Wingfield
Jefe jurídico de Global Partners Digital

Ioana Tuta
Asesora, Empresas y Derechos Humanos en el Instituto Danés de Derechos Humanos

Tulika Bansal
Asesora senior, Empresas y Derechos Humanos en el Instituto Danés de Derechos Humanos

AGRADECIMIENTOS
Los autores quisieran extender sus agradecimientos a todos quienes contribuyeron en la elaboración de este suplemento temático. En particular, a Sebastian Smart, quien ayudó a escribir el primer borrador de este documento. Los autores también quisieran reconocer la contribución de Equal Rights Trust y agradecer a su directora jurídica y de programas, Ariane Adam, por su contribución para resaltar los impactos discriminatorios de las actividades del sector tecnológico, al delinear las obligaciones de no discriminación de los actores estatales y privados y las responsabilidades de éstos últimos, además de brindar orientación sobre cómo dichas obligaciones y responsabilidades debieran abordarse en el proceso y contenido de un PAN.

Asimismo, los autores agradecen a quienes revisaron el borrador inicial de este suplemento temático, cuyos comentarios, retroalimentación y sugerencias fueron invaluables. En especial a: Dunstan Allison-Hope, Rémy Friedmann, Nora Götzmann, Emil Lindblad Kernell, Rikke Frank Jørgensen, Peter Micek, Daniel Morris, Isedua Oribhabor, Jason Pielemeier, Dr. Roxana Radu, Sabrina Rau, Elin Wrzoncki y a la Comisión Australiana de Derechos Humanos.

TRADUCCIÓN: María Francisca Díaz
Prueba de Lectura: Catalina Büchner

© Instituto Danés de Derechos Humanos

Wilders Plads 8K
DK-1403 Copenhague K
Teléfono +45 3269 8888
www.humanrights.dk

© Global Partners Digital

68 Hanbury St, Spitalfields
Londres E1 5JL, Reino Unido
www.gp-digital.org

Siempre que su reproducción no sea para uso comercial, esta publicación o partes de ella pueden ser reproducidas si se cita el autor y la fuente.

CONTENIDOS

INTRODUCCIÓN

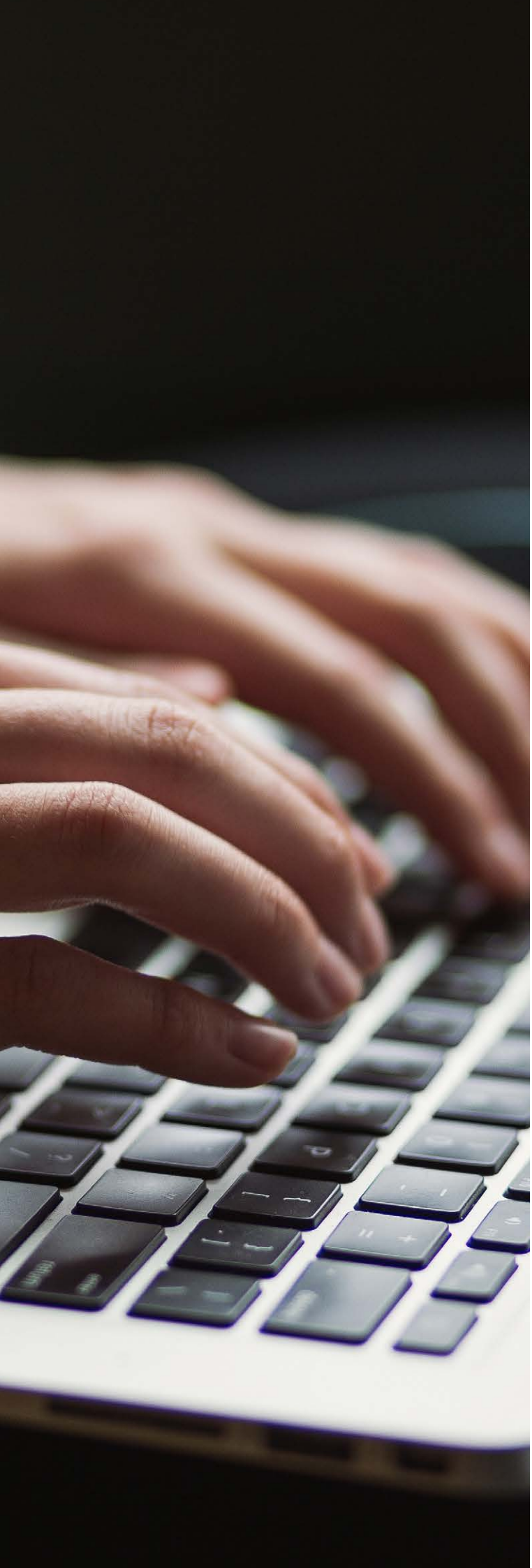
Las décadas recientes han sido testigo de los inmensos cambios que han sufrido las actividades humanas en casi todas las áreas como resultado de la innovación y desarrollo tecnológico, lo que conlleva importantes repercusiones en el ejercicio y disfrute igualitario de los derechos humanos. No cabe duda de que la tecnología digital ofrece una amplia variedad de oportunidades para mejorar el cumplimiento de los derechos humanos. En este sentido, la tecnología digital provee un mayor acceso a la educación y a la salud, y puede hacer que la disposición de éstos y otros servicios públicos sea más eficiente. Además, nuevas plataformas en línea permiten a las personas acceder y compartir noticias, información e ideas de forma mucho más fácil que antes, así como también permiten que comunidades y grupos se movilicen y se reúnan.

Al momento de escribir este suplemento temático, el mundo estaba paralizado casi por completo debido a la pandemia del COVID-19. Gracias a esta situación hemos visto cómo la sociedad se ha hecho cada vez más dependiente de la tecnología digital, ya sea para mantener el contacto con familiares y amigos, como con propósitos educacionales; para dialogar con colegas del trabajo y, quizás, lo más importante, para informarse.

Sin embargo, ciertas aplicaciones de tecnologías digitales pueden representar serios riesgos para los derechos humanos. Las actividades de las empresas tecnológicas en particular, los desarrolladores de softwares, las plataformas de medios sociales en línea, los motores de búsqueda y los proveedores de servicios de Internet han sido vinculados con efectos adversos sobre los derechos a la privacidad, la libertad de expresión, la libertad sindical, la no discriminación e incluso sobre el derecho a la vida.[1] Junto a los beneficios de la tecnología, los tiempos de crisis también revelan sus riesgos. De esta forma, el COVID-19 trajo consigo información engañosa sobre la propagación del virus en plataformas en línea, y también empresas tecnológicas con registros cuestionables sobre protección de datos y privacidad que ofrecieron “soluciones” a los gobiernos sobre cómo controlar a las personas y a la población.

Los impactos sobre los derechos humanos asociados con el desarrollo y despliegue de las tecnologías digitales han sido parte de la agenda pública por casi dos décadas, con especial atención sobre las operaciones y modelos de negocio de las grandes empresas, es decir, las empresas dominantes en el sector tecnológico. Sin embargo, las características del uso de las tecnologías digitales a gran escala traen consigo desafíos únicos para la protección y el respeto de los derechos humanos:

• Los impactos ocurren tanto a nivel nacional, como regional y mundial como resultado de que la infraestructura de Internet se encuentra interconectada globalmente, lo que significa que las respuestas a nivel nacional a menudo son ineficaces o insuficientes;



©Kaitly Baker

• los impactos son de largo alcance, con millones de usuarios (y otras personas) que enfrentan riesgos relativos a sus derechos humanos;

• el vínculo entre empresas tecnológicas y violaciones a los derechos humanos no es siempre evidente dada la naturaleza altamente especializada de sus actividades y la falta de transparencia en el desarrollo de tecnologías digitales, tales como la toma de decisiones automatizada o la inteligencia artificial;

• la identificación de los riesgos sobre los derechos humanos puede ser difícil debido al ritmo acelerado en el desarrollo e innovación en esta área;

• algunas de las cuestiones que trae consigo son nuevas y, por lo tanto, han sido abordadas de forma limitada en la jurisprudencia internacional y en el campo de la investigación legal sobre derechos humanos (cabe señalar que existe mayor énfasis y atención en el vínculo entre los derechos humanos y el sector tecnológico, entre otros, por parte de diferentes Relatores Especiales de la ONU).

La comprensión y el conocimiento general de los riesgos en derechos humanos vinculados con las tecnologías digitales han visto un incremento dentro del sector empresarial. Casos de alta connotación como los de Cambridge Analytica y las revelaciones de Snowden recibieron considerable atención, contribuyendo al vibrante debate político sobre las responsabilidades

de derechos humanos por parte tanto de los Estados como de las empresas en tiempos de big data y plataformas sociales. No obstante, el sector tecnológico se aborda de forma muy limitada en algunos Planes de acción nacionales de empresas y derechos humanos (PAN), si acaso se aborda (ver Sección 1.3), a pesar de que los PAN representan oportunidades para que los Estados propongan y presenten medidas a tomar para asegurar que los derechos humanos sean protegidos y respetados en el contexto de la actividad de las empresas tecnológicas. En general, existe una necesidad de mayor sinergia entre las empresas, los derechos humanos y las comunidades tecnológicas, lo que constituye un elemento crucial para fomentar la rendición de cuentas de las empresas tecnológicas, y diseñar marcos regulatorios y políticas adecuadas y compatibles con la normativa internacional de derechos humanos.

1.1 ACERCA DE ESTE SUPLEMENTO TEMÁTICO

En el contexto de los desafíos planteados en la introducción, este suplemento temático ha sido elaborado como una herramienta de apoyo para los actores estatales y otras partes interesadas en el desarrollo de los PAN, y tiene el objetivo de proporcionar orientación sobre la integración de los riesgos en derechos humanos asociados al sector tecnológico. Este documento complementa al Kit de herramientas sobre PAN desarrollado por la Mesa Redonda Internacional para la Rendición de Cuentas Empresarial (ICAR, por sus siglas en inglés) y el Instituto Danés de Derechos Humanos (el Kit de herramientas de ICAR-DIHR).[2]

El presente suplemento temático está dirigido, en primer lugar, a los Estados que se encuentren involucrados en el proceso de inicio, consulta, implementación o actualización de un PAN, y tanto en Estados donde se usen las tecnologías digitales desarrolladas por empresas (Estados anfitriones) como donde las empresas tecnológicas multinacionales estén domiciliadas o registradas (Estados de origen). Sin perjuicio de lo anterior, este suplemento también puede ser de utilidad para organizaciones de la sociedad civil, empresas tecnológicas y otras partes interesadas en los procesos de PAN.

Al primero de junio de 2020, 24 países han adoptado un PAN, lo que constituye un paso importante hacia la difusión e implementación de los Principios Rectores de la ONU (PRNU).[3] Los PRNU fueron respaldados por el Consejo de Derechos Humanos en el año 2011, y dejan en claro que las empresas tienen la responsabilidad de respetar los derechos humanos dondequiera que operen, independientemente de la capacidad de los Estados de cumplir con sus propias obligaciones en materia de derechos humanos (Principio 11).
Los PRNU también destacan el deber de los Estados de proteger

contra las violaciones de los derechos humanos que puedan ser cometidas por parte de las empresas. A tal efecto, los Estados deben adoptar las medidas apropiadas para prevenir, investigar, castigar y reparar dichos abusos mediante políticas adecuadas, actividades de reglamentación y sometimiento a la justicia (Principio 1). Los PRNU proporcionan una base normativa sólida para evaluar el impacto de las actividades de las empresas tecnológicas sobre los derechos humanos y desarrollar acciones y medidas políticas concretas para subsanar lagunas en materia de protección. Existen algunos PAN que ya hacen referencia a la tecnología digital y al sector tecnológico;[4] sin embargo, la mayoría de aquellas referencias son generales y carecen del nivel requerido para abordar la escala y el alcance de los impactos negativos sobre los derechos humanos generados en este sector.

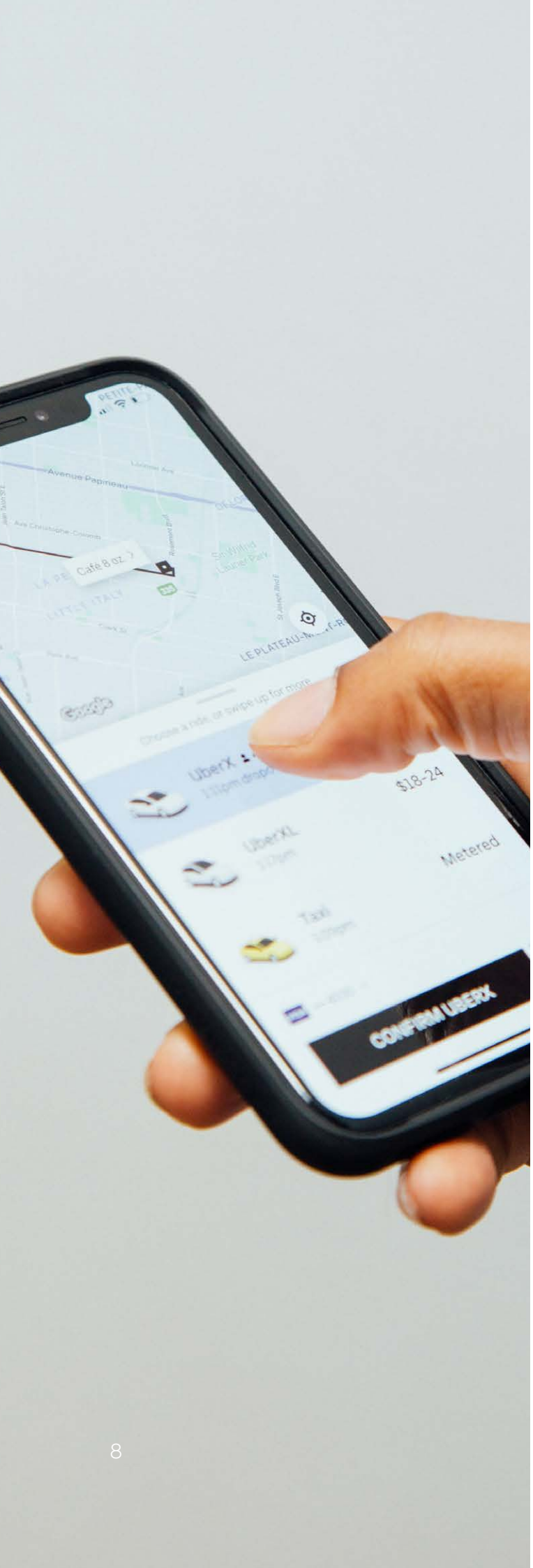
Si bien es cierto que todos los derechos humanos pueden verse afectados por las tecnologías digitales desarrolladas por empresas tecnológicas, el presente suplemento temático se enfoca en tres de los derechos más afectados: los derechos a la privacidad, a la libertad de expresión y a la igualdad y la no discriminación. Este documento será actualizado en el futuro con el fin de incluir cuestiones de derechos humanos relacionadas con otras tecnologías y el sector tecnológico, por lo que podría llegar a ser un espacio de convergencia para las organizaciones que trabajen en la intersección de la tecnología y los derechos humanos.

El presente suplemento temático se estructura en tres secciones.

El resto de la **Sección 1** proporciona información sobre el alcance del suplemento temático y un comentario sobre referencias actuales acerca del sector tecnológico en PAN.

La **Sección 2** se centra en la relación que existe entre el sector tecnológico y los derechos humanos, en especial entre el primero y los derechos a la privacidad, la libertad de expresión, y la igualdad y la no discriminación. Incluye una perspectiva general sobre el impacto que tienen las actividades de las empresas tecnológicas sobre los derechos mencionados anteriormente y se refiere a las tendencias normativas sobre esta materia.

La **Sección 3** comienza identificando la forma en que pueden incluirse las consideraciones relacionadas al sector tecnológico durante los procesos de PAN, con una lista de verificación de consideraciones para los Estados que estén interesados en abordar el impacto que las actividades relacionadas al sector tecnológico tienen sobre los derechos humanos dentro de sus PAN. Luego, se centra en la forma en que las consideraciones relacionadas al sector tecnológico pueden ser incluidas dentro de los contenidos de los PAN, e incluye una “Plantilla para una Evaluación Nacional de Línea de Base (ENLB) de PAN y el sector tecnológico”, la que contiene preguntas de orientación para evaluar las protecciones de derechos humanos existentes en relación con el



©Charles Deluvio

sector tecnológico, revelando lagunas en la implementación de los PRNU en ese aspecto. Las dos herramientas, la lista de verificación y la plantilla para una ENLB, deberían ser utilizadas en conjunto con el detallado Kit de herramientas de ICAR-DIHR para desarrollar, evaluar y ajustar los PAN.

Este suplemento temático debería servir como un conjunto de elementos mínimos para considerar durante el desarrollo de un PAN. Los actores estatales deben consultar siempre con las partes interesadas pertinentes que operen dentro y/o que puedan verse afectadas por el sector tecnológico a través del desarrollo e implementación de un PAN, para garantizar que éste sea lo más efectivo posible.

1.2. ALCANCE DEL SUPLEMENTO TEMÁTICO

1.2.1. EN CUANTO A LAS EMPRESAS

El alcance de este suplemento temático está contenido en el “sector de la tecnología” (o “sector tecnológico”). No existe una definición única o categórica sobre este tipo de industrias o empresas, y el hecho de que hoy la mayoría de las empresas, sin importar su sector, tamaño o ubicación, usan Internet y las tecnologías digitales para desarrollar y distribuir sus productos y servicios, dificulta la elaboración de una definición clara. En efecto, es posible

que una empresa de logística utilice un software de gestión específico, o que un distribuidor pueda proporcionar productos a través de una plataforma en línea o pueda promocionar sus productos en línea; o que una institución financiera pueda utilizar servicios de la computación en la nube para almacenar y administrar grandes cantidades de datos.

Por otra parte, la definición del sector puede ser polémica en casos que involucren el cumplimiento de normas regulatorias. Por ejemplo, empresas que pertenecen a la "economía de pequeños encargos" o "economía gig", tales como Uber y Airbnb, han sido cuestionadas por autodefinirse como empresas plataforma de intermediación digital, lo que les permite evadir el cumplimiento de requerimientos regulatorios más estrictos que se aplican a empresas tradicionales de transporte y de hotelería. En distintas cortes en todo el mundo se han conocido casos para decidir si es que Uber es un servicio digital o si es una empresa tradicional que utiliza tecnología digital.[5] En un juicio histórico en 2017, el Tribunal de Justicia de la Unión Europea dictaminó que Uber es una empresa de transporte y no un servicio de la sociedad de la información y, por lo tanto, está sujeta a las normas aplicables a los taxistas profesionales en materia de licencias.

En este contexto, el presente informe no plantea una definición específica sobre el sector tecnológico, pero sí destaca que de forma general éste puede ser entendido como un sector que agrupa a industrias cuyos modelos de negocios permiten el acceso y el funcionamiento de la Internet y las tecnologías digitales, incluyendo el desarrollo y distribución de productos, servicios y contenidos digitales. Esta interpretación general podría significar que el sector tecnológico incluye compañías de telecomunicaciones, proveedores de servicios de Internet, compañías de nombres de dominio tales como registros y registradores; compañías de Internet que proveen contenido; comunicación y servicios tales como motores de búsqueda, plataformas de redes sociales, aplicaciones de mensajería; y compañías de hardware y software, incluyendo proveedores de equipos de red.

Teniendo en cuenta el enfoque limitado de derechos humanos de este suplemento temático, es decir, los derechos a la privacidad, la libertad de expresión y la igualdad y la no discriminación (véase Sección 1.2.2), este informe se centra y proporciona ejemplos principalmente de aquellas industrias y empresas donde cuestiones relativas a los derechos humanos mencionados anteriormente han sido ampliamente documentadas y donde son especialmente importantes.

El enfoque de la Sustainability Accounting Standards Board para definir el sector tecnológico

La **Sustainability Accounting Standards Board** (SASB) es una organización independiente que establece estándares de contabilidad basados en la sostenibilidad. La SASB identifica cinco industrias en el sector de la tecnología y la comunicación: servicios de fabricación de productos electrónicos y elaboración de diseños originales; hardware; medios y servicios de Internet; semiconductores; servicios de software y tecnologías informáticas; y telecomunicaciones. Dada la creciente integración y convergencia en este sector, es posible que una empresa pueda pertenecer de forma simultánea a más de una de estas industrias. Por ejemplo, la empresa Google es activa en múltiples segmentos empresariales, ya que es un motor de búsqueda, un desarrollador de software y una empresa de infraestructura de Internet a la vez.

El impacto en los derechos humanos más allá del sector tecnológico

Aunque el foco de este suplemento temático se centra en el impacto que las actividades de las empresas del sector tecnológico tienen sobre los derechos humanos, cualquier compañía que utilice, implemente o dependa de la tecnología digital puede, con ello, generar impactos negativos potenciales sobre los derechos humanos.

Por ejemplo, el uso de tecnología de vigilancia por parte de compañías para controlar a sus empleados en el trabajo puede constituir una violación al derecho a la privacidad. Una encuesta llevada a cabo por Gartner develó que casi un cuarto de las organizaciones a nivel mundial utiliza datos de tráfico de sus empleados, y un 17% supervisa el uso de los datos de los computadores del trabajo. Algunas empresas controlan el uso de medios sociales por parte de sus empleados, incluso cuando estos se encuentran fuera del trabajo y existen casos donde los empleados han visto sus contratos terminados por el hecho de expresar sus opiniones a través de medios sociales.

El aumento del teletrabajo debido al COVID-19 llevó a algunos empleadores a utilizar herramientas digitales nuevas para monitorear a su personal de forma remota, incluyendo el control de las páginas web que éstos visitan. Así, por ejemplo, algunos empleadores utilizan productos digitales, tales como Sneek, programa que toma fotografías periódicamente a través de la cámara del ordenador portátil para asegurarse de que los empleados lo utilizan durante la jornada laboral.

Otro ejemplo es el creciente uso de inteligencia artificial en variados sectores, como es el caso del sector de servicios financieros, donde se utiliza para tomar decisiones respecto a la aptitud de los clientes para obtener préstamos o para determinar las tasas de interés. Existe evidencia sobre el uso de decisiones automatizadas en dichas instancias, lo que conduce a conclusiones discriminatorias que, incluso, se basan en variables como la raza y el origen étnico.

A pesar de este enfoque, muchos de los elementos de este suplemento temático, en particular aquellos relacionados a la privacidad y protección de datos, también servirán para otras empresas que usen tecnología digital de alguna manera, por lo que el impacto que tendrá un PAN desarrollado de acuerdo con la presente guía tendrá un mayor alcance.

1.2.2. EN CUANTO A LOS DERECHOS HUMANOS

La primera parte de este suplemento temático se centra en tres de los derechos humanos que han sido frecuentemente considerados respecto a los impactos de las actividades del sector tecnológico: los derechos a la privacidad, a la libertad de expresión y a la igualdad y no discriminación. Como se ha mencionado anteriormente, este suplemento temático será actualizado para así incluir otras cuestiones de derechos humanos relacionadas al sector tecnológico, esperando que se convierta en un recurso mucho más completo.

Los derechos a la privacidad y la libertad de expresión son especialmente importantes, dado que son considerados como derechos que permiten el goce de otros derechos humanos. Por ejemplo, el derecho a la privacidad permite el libre desarrollo de la personalidad e identidad de una persona, así como también contribuye a su habilidad para participar en la vida política, económica, social y cultural.[6] Por otro lado, tomando en cuenta el anonimato que proporcionan ciertas plataformas en línea o la garantía de confidencialidad que ofrecen herramientas de cifrado, las personas pueden sentirse más libres para discutir temas personales o sensibles, así como para participar en debates sobre cuestiones controversiales donde hablar abiertamente podría conducir hacia episodios de acoso o violencia.

El goce de la libertad de expresión incluye la habilidad de difundir, buscar y recibir información, y opera como catalizador para el cumplimiento de ciertos derechos asociados, como el derecho a la libertad de asociación y de reunión pacífica, el derecho a participar en la dirección de asuntos públicos, el derecho a la educación, el derecho a participar en la vida cultural, y el derecho a gozar de los beneficios del progreso científico y sus aplicaciones. Por ejemplo, las personas no solo pueden comunicarse a través de plataformas en línea, sino que también pueden organizar protestas o movimientos masivos. Asimismo, en la actualidad se encuentra disponible una amplia gama de plataformas educacionales en línea, dirigidas a personas cuyas oportunidades de aprovechar formas de educación más tradicionales se encuentran limitadas.

La no discriminación constituye un principio básico y fundamental que tiene relación con la protección de todos los derechos humanos.[7] En este sentido, el derecho internacional de los derechos humanos reconoce que, para respetar y garantizar los derechos humanos, se requiere la no discriminación. Asimismo, los Principios

Rectores enfatizan que deben ser aplicados de manera no discriminatoria, y en el comentario del Principio 3 se señala que el incumplimiento de las leyes vigentes sobre discriminación que directa o indirectamente regulan la observancia de los derechos humanos por las empresas constituye una laguna legal frecuente en la práctica de los Estados.

La interrelación de todos los derechos humanos es bidireccional, lo que significa que las consecuencias negativas sobre los derechos a la privacidad, a la libertad de expresión y a la igualdad y no discriminación pueden propiciar restricciones sobre otros derechos humanos.

Los derechos a la privacidad, la libertad de expresión, y la igualdad y la no discriminación

Hace tiempo que el **derecho a la privacidad** es reconocido en el derecho internacional de los derechos humanos y se inspira en el Artículo 12 de la Declaración Universal de Derechos Humanos (DUDH). Además, el Pacto Internacional de Derechos Civiles y Políticos (ICCPR por sus siglas en inglés) señala en su Artículo 17 que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación". Y continúa estableciendo que "toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

El **derecho a la libertad de expresión** puede ser definido de manera general como el derecho de una persona a emitir opiniones sin ser objeto de injerencia alguna, y a buscar, recibir y difundir informaciones o ideas a través de cualquier medio y sin consideración de fronteras. El Artículo 19(2) del ICCPR, haciendo eco del Artículo 19 de la DUDH, dispone que "Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección".

El derecho a la libertad de expresión está muy ligado al derecho de libertad de opinión. El Artículo 19(1) del ICCPR (nuevamente haciendo eco del contenido del Artículo 19 de la DUDH), ordena que "nadie podrá ser molestado a causa de sus opiniones".

El derecho a la libertad de opinión es un derecho absoluto, es decir, ninguna interferencia hacia este derecho puede ser justificada. Este no es el caso de los derechos a la privacidad y la libertad de expresión, los que son derechos no absolutos. Ellos pueden ser limitados o restringidos en ciertas circunstancias cuando:

- Existe un fundamento jurídico claro;
- se hace en cumplimiento de un objetivo legítimo; y
- es una respuesta necesaria y proporcionada para cumplir ese objetivo.

Los derechos a la igualdad y la no discriminación también han sido largamente reconocidos en el derecho internacional de los derechos humanos. En efecto, el

derecho a la no discriminación sustenta el derecho internacional de los derechos humanos con el Artículo 2(1) del ICCPR, donde se exige que los derechos reconocidos en el Pacto sean respetados "sin distinción alguna" y se prohíbe, por ende, la discriminación en el goce de todos los derechos humanos (en línea con los Artículos 2 y 7 de la DUDH). El Artículo 26 del Pacto, sin embargo, establece el derecho autónomo a la igualdad basándose en el Artículo 7 de la DUDH, declarando que:

- Todas las personas son iguales ante la ley;
- todas las personas tienen derecho sin discriminación a igual protección de la ley; y
- los Estados deben asegurar que la ley prohibirá toda discriminación y garantizará a todas las personas protección igual y efectiva contra cualquier discriminación de cualquier índole.

El Comité de Derechos Humanos de la ONU señala que el Artículo 26 del ICCPR "prohíbe la discriminación de hecho o de derecho en cualquier esfera" y, por lo tanto, no se limita a aquellos derechos contemplados en el Pacto. El Comité de Derechos Humanos de la ONU señala también que para cumplir sus obligaciones relativas a la no discriminación, los Estados deben adoptar una legislación global de lucha contra la discriminación. En aquellos Estados donde se haya implementado el derecho a la no discriminación, las empresas del sector tecnológico, así como las del sector privado en general, tendrán la obligación legal de no discriminar en ningún ámbito.

Al igual que los derechos a la privacidad y la libertad de expresión, los derechos a la igualdad y la no discriminación no son derechos absolutos. La diferenciación de trato solo será permisible, sin embargo, si los criterios para dicha diferenciación son razonables y objetivos y si se lleva a cabo con fines legítimos.

1.3. COMENTARIOS SOBRE PAN ACTUALES

Hasta el primero de junio de 2020, 24 Estados han adoptado un PAN.[8] De esos PAN, diez hacen referencia al sector tecnológico y, de esos diez, cinco contienen acciones específicas y compromisos relacionados al mencionado sector. Los otros cinco se limitan a señalar que existen impactos negativos sobre los derechos humanos relacionados con el sector tecnológico.

El texto de los diez PAN que mencionan al sector tecnológico se encuentra en el Anexo 1 de este suplemento temático, junto con detalles de implementación de acciones, donde sea relevante y se encuentre disponible.

En resumen, los puntos de acción en los cinco PAN que asumen compromisos relacionados al sector tecnológico son variados: El de Finlandia se refiere a una mesa redonda sobre protección de datos; aquel de Polonia aborda la regulación de la responsabilidad legal de los intermediarios; el de Reino Unido contiene orientaciones para exportar información y tecnología de las comunicaciones; el de los Estados Unidos se refiere a mecanismos que ayudan a identificar lecciones aprendidas y mejores prácticas relacionadas a empresas que promuevan los derechos humanos en línea; y, finalmente, el de Tailandia se dedica al desarrollo de planes y medidas para asistir a trabajadores reemplazados por la tecnología. Solo en uno de estos casos (el de Reino Unido) se detalla cómo estos compromisos han sido implementados por el Estado. [9]

Es posible formular tres observaciones en base al lenguaje y a los compromisos contenidos en los PAN actuales:

1. El amplio espectro de riesgos relativos a los derechos humanos que emanan de las actividades del sector tecnológico, en particular sobre la privacidad, la libertad de expresión y la igualdad y la no discriminación, no son considerados cabalmente en ninguno de los PAN publicados hasta la fecha. Los PAN que consideran al sector tecnológico tienden a examinar solo un limitado aspecto de los riesgos de derechos humanos que presenta el sector, tales como la privacidad (Finlandia), la libertad de expresión (Polonia) o el derecho al trabajo (Tailandia). El derecho a la no discriminación es considerado principalmente en relación con el empleo, mientras que el amplio espectro de efectos discriminatorios sobre el uso de nuevas tecnologías digitales no se aborda. Si bien esto puede reflejar una priorización por parte del Estado hacia cuestiones más graves en sus PAN, también puede representar un incumplimiento o fracaso en considerar de forma integral la diversa gama de impactos negativos sobre los derechos humanos que emanan del sector tecnológico.

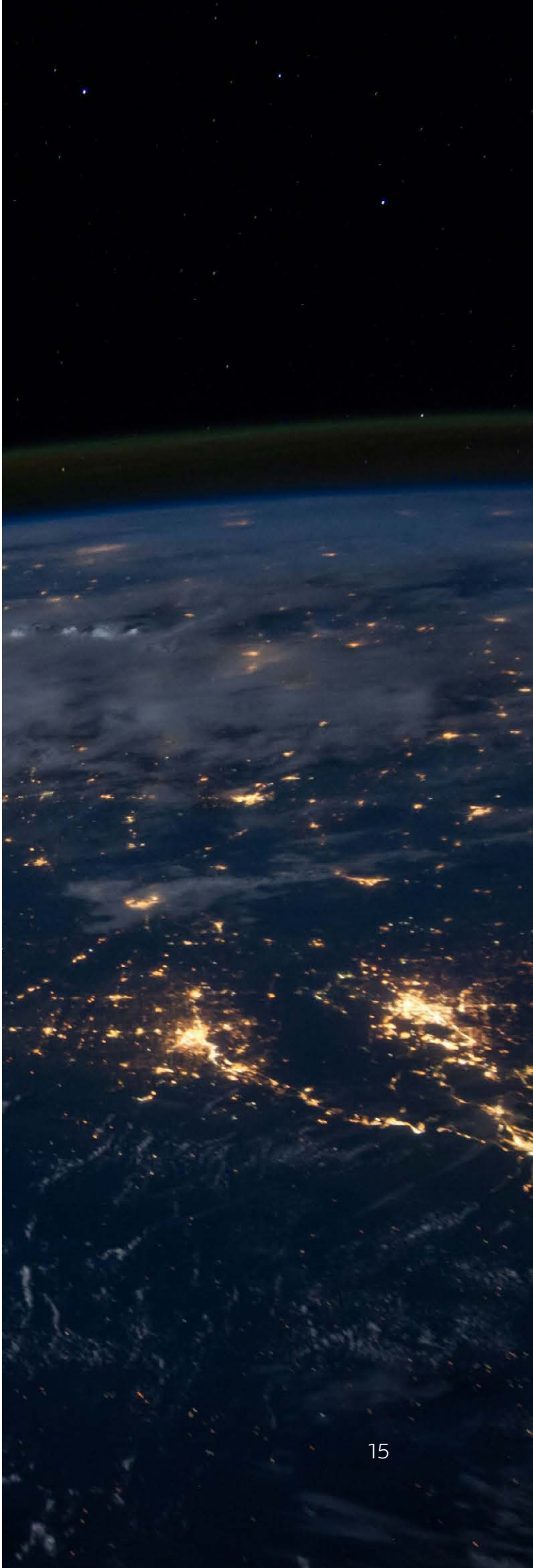
2. Ninguno de los compromisos relacionados al sector tecnológico descritos en los cuatro PAN que los contienen pueden ser considerados como totalmente SMART (específicos, medibles, alcanzables, relevantes y acotados en el tiempo).[10] Asimismo, ninguno de los cinco PAN proporciona detalles sobre plazos para cumplir los compromisos o sobre los fondos que serían provistos. Tampoco alguno de los cuatro proporciona detalles sobre cómo las conclusiones podrían ser publicadas y su impacto monitoreado.

3. Ninguno de los compromisos relacionados al sector tecnológico descritos en los PAN aborda el Pilar III de los PRNU, el que se enfoca en el acceso a mecanismos de reparación. El foco en estos cinco PAN se centra en el Pilar I: por ejemplo, en la regulación de la responsabilidad legal de los intermediarios; y en el Pilar II: por ejemplo, en la orientación sobre consideraciones de derechos

humanos cuando se exportan productos tecnológicos y comparten mejores prácticas por parte de políticas corporativas que promueven los derechos humanos en línea.

2. EL SECTOR TECNOLÓGICO E IMPACTOS SOBRE LOS DERECHOS HUMANOS

Como se mencionó en la Sección 1, las empresas tecnológicas, y los productos y servicios digitales que desarrollan y distribuyen, ofrecen un abanico de oportunidades para apoyar el cumplimiento y el goce de los derechos humanos. El desarrollo de productos de cifrado reforzado ayuda a proteger el derecho a la privacidad, manteniendo los datos personales y las comunicaciones seguras. Esto es especialmente importante, sobre todo para grupos que se encuentran en riesgo de sufrir tratos discriminatorios por parte del Estado o de actores privados. Las plataformas de medios sociales proporcionan nuevas formas para que las voces de mil millones de personas alrededor del mundo sean escuchadas, incluyendo las de grupos marginados, lo que hace que la comunicación y el compartir información e ideas sea más fácil que nunca, y fortalece el goce igualitario del derecho a la libertad de expresión.



© Nasa - Unsplash

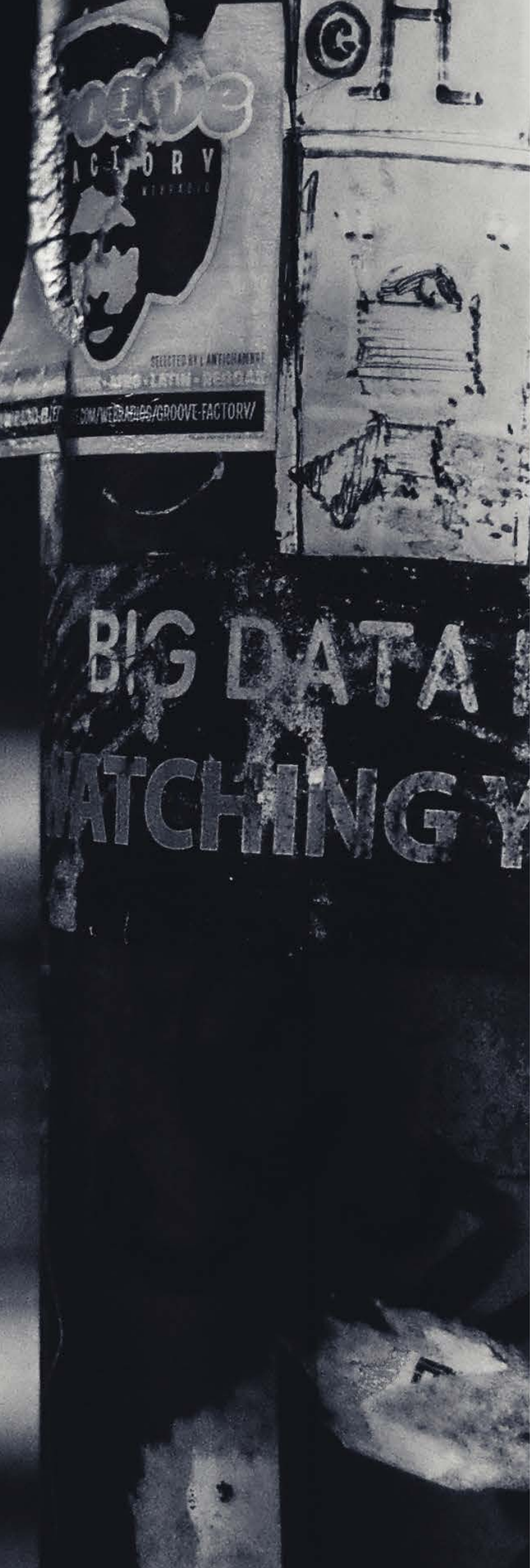
Además, como se ha señalado en la Sección 1.2.2., los derechos a la privacidad y la libertad de expresión actúan como "guardianes" que protegen el goce igualitario de otros derechos asociados. Dichos productos y servicios también traen consigo otros beneficios para los derechos humanos, ya que permiten a las víctimas de violaciones de derechos humanos denunciar y generar consciencia de estas, así como también buscar y obtener reparación.[11]

Sin embargo, estas compañías y sus productos y servicios pueden, a su vez, crear riesgos asociados sobre los derechos a la privacidad, la libertad de expresión y la igualdad y la no discriminación. En este sentido, un PAN que considera al sector tecnológico puede ayudar a evitar o mitigar dichos riesgos.

2.1. EL DERECHO A LA PRIVACIDAD (INCLUYENDO EFECTOS DISCRIMINATO-RIOS)

El modelo de negocio de muchas empresas tecnológicas se basa en la recolección y el procesamiento de grandes cantidades de datos personales ligados al comportamiento de las personas en línea y fuera de línea. A menudo, dichos datos son utilizados para crear perfiles altamente sofisticados que incluyen asuntos personales y confidenciales sobre la identidad de las personas. Aunque con frecuencia estos datos se han utilizado con propósitos comerciales, tales como activar publicidad dirigida, esta práctica en sí misma ha generado inquietudes relacionadas con la privacidad, la libertad de expresión y la igualdad y la no discriminación.[12] De igual manera, estos datos se han utilizado para seguir y vigilar a las personas por parte de las empresas y, a veces, también han sido facilitados a o hackeados por actores estatales, como lo son las fuerzas de orden y seguridad. Con el advenimiento de nuevas tecnologías, tales como el 5G, la Internet de las Cosas, y la inteligencia artificial (IA), la cantidad de datos recolectados va en aumento, lo que significa que la prevalencia de dichos usos de la información también se extenderá.

Este tipo de modelo de negocio ha sido objeto de escrutinio por los impactos negativos, reales o potenciales, sobre los derechos a la privacidad y la igualdad y la no discriminación. En este sentido, los datos personales (incluyendo metadatos), ya sea que se recopilen y compartan con o sin el consentimiento de las personas involucradas, no solo se utilizan en sí mismos, sino que se comparten y correlacionan con otras fuentes de datos para crear perfiles individuales y grupales aún más detallados. La consolidación de diferentes conjuntos de datos, incluso aparentemente anónimos, plantea dudas sobre los derechos de los usuarios a saber, consentir y ejercer el control sobre



© Ev - Unsplash

sus datos personales de acuerdo con su derecho a la privacidad. Además, como la tecnología se vuelve cada vez más poderosa, es cada vez más fácil recolectar y procesar "big data", es decir, grandes conjuntos de datos. De acuerdo con el Relator Especial de la ONU sobre el derecho a la privacidad, "la tendencia del Big Data de entrometerse en las vidas de las personas al dar a conocer su yo informacional en detalle a quienes recopilan y analizan sus rastros de datos, está fundamentalmente en conflicto con el derecho a la privacidad y los principios respaldados para proteger ese derecho".[13] [cita traducida]

El Relator Especial también destacó que se reconoce el derecho a la privacidad en instrumentos internacionales como "un derecho fuertemente vinculado a los conceptos de dignidad humana y al desarrollo libre e ilimitado de la personalidad de las personas".[14] La capacidad de mantener distintos contextos en los cuales se divulgue o se encubra las identidades sin datos de vigilancia puede ser crucial para los grupos en riesgo de discriminación. Por ejemplo, puede ser vital para aquellas personas que pertenezcan a la comunidad LGBTI que vivan en un país donde las relaciones entre personas del mismo sexo sean estigmatizadas o consideradas ilegales.[15]

Los conjuntos de datos son frecuentemente analizados por algoritmos y por otras formas de inteligencia artificial, tecnologías que se están volviendo rápidamente parte de la infraestructura crítica de

nuestras sociedades. Sin embargo, recién comenzamos a entender el impacto de la inteligencia artificial, el big data y las tecnologías asociadas sobre los derechos humanos.[16] Dichas tecnologías pueden conducir hacia prácticas discriminatorias de diferentes formas,[17] incluyendo recibir capacitación sobre la base de información o muestras sesgadas y, por lo tanto, reproducir patrones de discriminación existentes.[18]

Por ejemplo, Reuters informó en 2018 que Amazon dejó de hacer uso de un sistema de selección de personal que utilizaba inteligencia artificial porque el sistema presentaba sesgos en contra de las mujeres. De acuerdo con el informe, "la compañía se dio cuenta de que el nuevo sistema no estaba calificando a los candidatos a las vacantes de desarrollador de software y otras posiciones técnicas de forma neutra".[19] Basado en los datos procesados, "el sistema de Amazon se enseñó a sí mismo que eran preferibles los candidatos varones".[20]

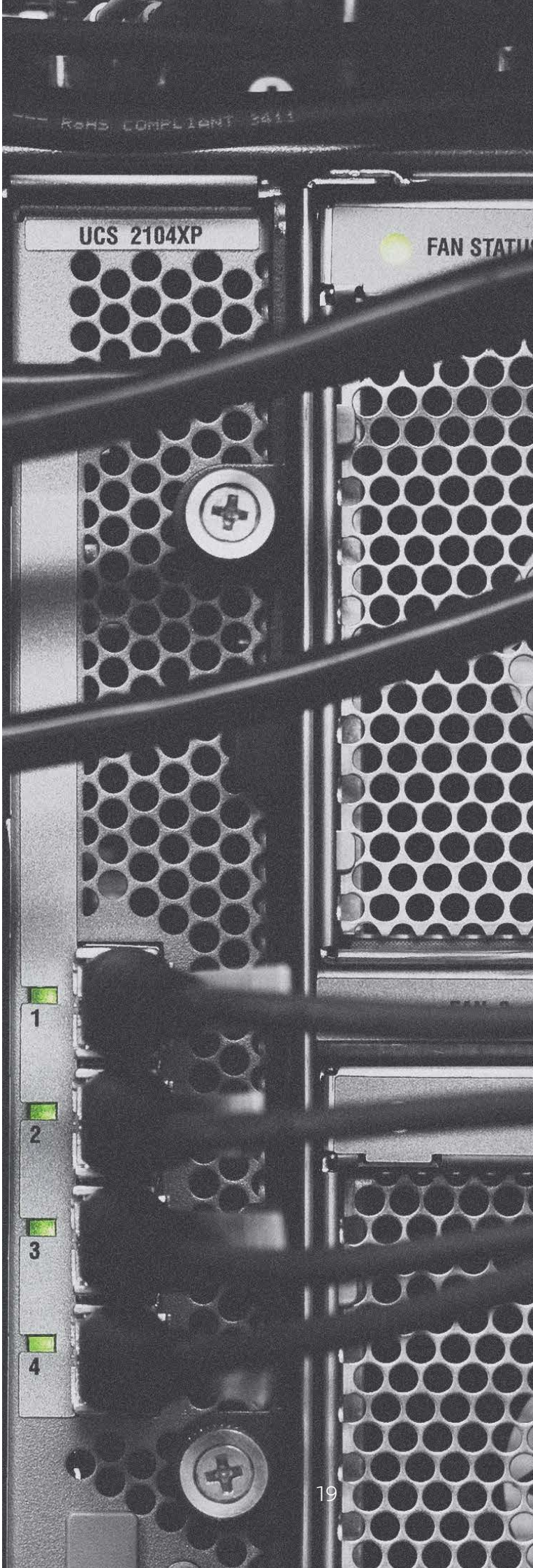
La compra y venta de información por parte de los "corredores de datos" con fines comerciales tales como publicidad, puntaje de crédito y análisis de riesgos para seguros, han sido vinculadas a la falta de transparencia, la conservación de datos de forma indefinida y resultados discriminatorios por parte de algoritmos.[21] En este sentido, un estudio realizado por la organización ProPublica en 2017 reveló que los anunciantes de Facebook podían excluir a ciertos grupos en sus anuncios de rentas habitacionales, incluyendo a afroestadounidenses, personas interesadas en rampas para sillas de ruedas e hispanohablantes, a pesar de que la compañía anunció que había construido un sistema para identificar y descartar anuncios discriminatorios.[22]

En algunos Estados dentro de los Estados Unidos, los sistemas de justicia penal utilizan un programa llamado COMPAS (por su nombre en inglés Correctional Offender Management Profiling for Alternative Sanctions, que en español puede traducirse como Administración de Perfiles de Criminales para Sanciones Alternativas del Sistema de Prisiones) para ayudar a los jueces a determinar si una persona condenada por la comisión de un delito podría ser supervisada fuera de prisión en lugar de ir a la cárcel. Investigaciones periodísticas llevadas a cabo en 2016 demostraron que COMPAS presentaba sesgos raciales: las personas afrodescendientes tenían casi el doble de posibilidades que las personas blancas de ser catalogadas como de alto riesgo, sin presentar reincidencia y, por otra parte, las personas blancas tenían muchas más posibilidades de ser catalogadas como de bajo riesgo, pero luego cometían nuevos crímenes. [23]

La recolección masiva y poco transparente de vastas cantidades de información, incluyendo datos personales, puede crear riesgos de violaciones de datos personales, así como uso indebido de esos datos y discriminación. El escándalo de Cambridge Analytica reveló que Facebook permitió la recopilación de

datos de 87 millones de usuarios, los que, posteriormente, fueron utilizados para tratar de influir en los resultados de la campaña presidencial de los Estados Unidos de 2016.[24] Por su parte, la violación de datos de Yahoo en 2013 afectó a tres mil millones de cuentas, poniendo en riesgo información personal de millones de sus usuarios con informes de que la información robada fue utilizada por gobiernos para identificar a las personas.[25]

Las empresas tecnológicas, incluyendo a los proveedores de servicios de Internet y los puntos de intercambio de Internet, se han visto bajo presión para compartir datos personales con agencias de seguridad nacionales involucradas en vigilancia digital, lo que conllevaría impactos negativos sobre la privacidad, la igualdad y la no discriminación y otros derechos humanos. Por ejemplo, en los Estados Unidos el programa de vigilancia llamado PRISM, denunciado como resultado de las filtraciones de Snowden del año 2013, fue objeto de críticas por acumular grandes cantidades de datos sobre estadounidenses que no eran objetivos de espionaje ni tampoco significaban amenazas a la seguridad. Además, los datos recopilados de esa manera fueron utilizados para identificar e investigar a los sospechosos violando el derecho a un juicio con las debidas garantías.[26] Numerosas demandas legales en contra de empresas tecnológicas se encuentran abiertas en diferentes jurisdicciones por facilitar violaciones a los derechos humanos perpetradas por Estados como resultado de la



© Kvistholt

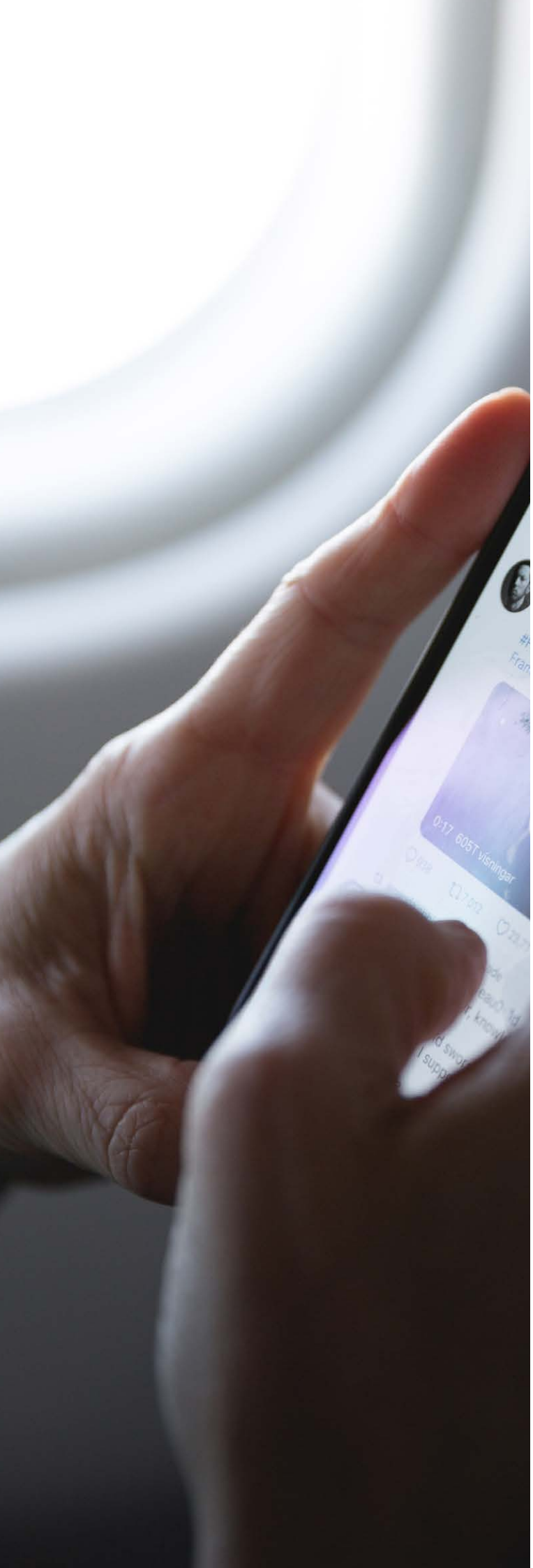
recopilación de datos a través de técnicas de vigilancia digital.[27] Los grupos en riesgo de discriminación son especialmente vulnerables al intercambio masivo de conjuntos de datos para vigilancia estatal. Por ejemplo, el big data impulsó la represión por parte del Estado chino contra la etnia uigur y otras minorías étnicas en la región de Xinjiang.[28]

Marcos e iniciativas

El reporte "Freedom on the Net" publicado el año 2018 por la Freedom House demostró que desde el mes de junio del año 2017, 18 gobiernos de los 65 Estados analizados revisaron o promulgaron legislación o directivas nuevas para incrementar la vigilancia estatal en línea.[29] Algunos Estados exigieron a las empresas tecnológicas almacenar la información de sus ciudadanos en servidores locales con el objetivo de que los registros sean más fáciles de acceder para las agencias de seguridad nacionales o para protegerlos de robo o explotación.[30] Ante esta situación, los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones fueron creados por un grupo de diversas partes interesadas con el objetivo de clarificar cómo el derecho internacional de los derechos humanos se aplica a las tecnologías y técnicas de comunicaciones actuales.[31] Las empresas tecnológicas han unido fuerzas para rechazar las peticiones de los gobiernos para recopilar datos de sus usuarios. A través de la coalición "Reform Government Surveillance", compañías tales como Google, Apple, Facebook, Dropbox, Twitter y LinkedIn han solicitado la reforma de leyes y prácticas sobre vigilancia gubernamental y sobre el acceso a su información por parte de los gobiernos del mundo.[32]

Algunos Estados han planteado inquietudes sobre los desafíos que representan para la aplicación de la ley las sofisticadas herramientas de cifrado y los productos desarrollados por empresas tecnológicas para proteger la seguridad de sus usuarios en línea. Por ejemplo, en 2018, los Estados miembros del grupo denominado Five Eyes, agencia de inteligencia compuesta por el Reino Unido, los Estados Unidos, Canadá, Australia y Nueva Zelanda, hicieron pública una declaración conjunta llamando a las empresas tecnológicas a establecer soluciones de acceso legales de forma voluntaria para los contenidos cifrados.[33]

La proliferación de riesgos digitales para la seguridad y protección de datos ha resaltado las deficiencias de varios marcos de protección de datos. A nivel mundial, la mayoría de las legislaciones sobre privacidad y protección de datos de información han sido informadas por los principios de la protección de datos de las Directrices de la OCDE sobre Protección de la privacidad y flujos transfronterizos de datos personales adoptadas en 1980 (actualizada en 2013) y por el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa adoptado en 1981 (Convenio n°



© Marten Bjork

108). Como resultado, muchos Estados se encuentran revisando o adoptando nueva legislación sobre protección y privacidad de datos.

Mientras que más de 100 Estados han adoptado de alguna forma legislación sobre protección de datos, el Reglamento general de protección de datos de la UE (RGPD) es el de mayor alcance adoptado hasta ahora (véase el Cuadro 4). Aclamado por su potencial de fortalecer la protección de datos así como el derecho a la privacidad, el RGPD es parte de un plan regulador mayor que está siendo desarrollado por la UE, y que incluye la Ley de Ciberseguridad y la revisión de la Directiva sobre la privacidad y las comunicaciones electrónicas.[34] También incluye una directiva sobre el procesamiento de datos personales en lo que respecta a su tratamiento por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.[35]

Según el Comité Europeo de Protección de Datos, más de 89.000 violaciones de datos fueron registradas por las autoridades supervisoras durante el primer año que el RGPD entró en vigor en mayo de 2018.[36] Google fue sancionada por la Comisión Nacional de Informática y Libertades con una multa récord de 50 millones de euros por violar la nueva ley.[37]

Reglamento general de protección de datos de la UE (Reglamento (UE) 2016/679)

El Reglamento general de protección de datos (RGPD) entró en vigor en mayo de 2018 y se aplica a todos los individuos, organizaciones y empresas que recopilen, conserven y traten datos de individuos dentro de la UE. Los datos personales son cualquier información relativa a una persona física viva, identificada o identificable. Además, son protegidos independientemente de la tecnología utilizada para su tratamiento o su conservación y se aplica tanto al tratamiento automatizado como manual. El RGPD exige que las compañías cuenten con el consentimiento explícito de las personas ("interesados") de quienes obtengan datos, y exige que formulen políticas de privacidad "que sean fácilmente accesibles y fácil de entender, y que se utilice un lenguaje sencillo y claro". Un aspecto relevante es que, para cumplir con lo provisto por el RGPD, el consentimiento no debe estar oculto en los términos y condiciones. Asimismo, en los casos donde el procesamiento de datos tenga múltiples propósitos, el consentimiento debe ser obtenido para todos y cada uno de ellos.

El RGPD también trae consigo más transparencia, al exigir a las empresas que informen a los usuarios si es que sus datos son enviados fuera de la UE, si los datos recopilados son usados con diferentes fines que los originales y si las decisiones tomadas usando sus datos es automatizada. Incluso da la posibilidad a los usuarios de impugnar las decisiones de las empresas. El Reglamento confiere a las personas mayores derechos para acceder a los datos sobre sí mismas, para ser notificadas rápidamente en caso de violaciones de cualquier índole y al "derecho al olvido" (derecho a suprimir datos personales).

El RGPD también crea mecanismos de supervisión y aplicación más estrictos, al proporcionar a las autoridades nacionales encargadas de la protección de datos el poder de imponer multas por infracciones a las empresas por una cuantía equivalente al 4% como máximo de su volumen de negocio global. Igualmente, este instrumento incentiva a las empresas a cooperar a través del Comité Europeo de Protección de Datos, el cual proporciona orientación e interpretación y adopta decisiones vinculantes en casos transfronterizos.

El RGPD también introduce algunas disposiciones nuevas, tales como la exigencia de evaluación de impacto relativa a la protección de datos en situaciones con probabilidad de resultar en alto riesgo para los derechos y libertades de las personas, y a los derechos a portabilidad de datos y a no estar sujeto a decisiones basadas solamente en tratamientos automatizados que producen efectos jurídicos u otros relativos a la persona.

El RGPD ha informado legislación similar en otras jurisdicciones, tales como la Ley de privacidad del consumidor de California y leyes de protección de datos en Argentina, Brasil e Indonesia. Como ya se ha mencionado en esta Sección, nuevas tecnologías como el 5G, la Internet de las cosas, y la inteligencia artificial solo van a acelerar el alcance y la escala de la recolección de datos y confundir aún más la distinción entre datos personales y no personales. Los entes reguladores y los responsables de formular políticas públicas están explorando cada vez más soluciones que combinen dominios regulatorios distintivos previos, tales como la protección al consumidor, normas de competencia y protección de datos, con el fin de adelantarse a la curva de la innovación digital.

A pesar de que las leyes y políticas de protección de datos van, de alguna manera, en la dirección correcta en cuanto a la mitigación de los daños a los derechos humanos por parte de las nuevas tecnologías, incluyendo la inteligencia artificial y el big data, muchas de estas tecnologías están siendo usadas con mayor frecuencia por Estados que no han adoptado leyes generales contra la discriminación. Lo anterior implica que sus marcos legales actuales no son suficientes para prevenir la aplicación discriminatoria de las tecnologías mencionadas.[38]

La Declaración de Toronto sobre la protección del derecho a la igualdad y la no discriminación en los sistemas de aprendizaje automático se lanzó gracias a un grupo de organizaciones no gubernamentales en 2018, para dar respuesta, específicamente, a inquietudes en torno a riesgos de discriminación. La Declaración de Toronto exhorta a los gobiernos y a las empresas a que aseguren que las tecnologías de aprendizaje automático respeten los principios de igualdad y no discriminación.[39]

2.2. EL DERECHO A LA LIBERTAD DE EXPRESIÓN (INCLUYENDO EFECTOS DISCRIMINATORIOS)

Si bien es cierto que las plataformas de medios sociales, los servicios de mensajería y los motores de búsqueda proporcionan nuevos espacios para que las personas ejerzan su derecho a la libertad de expresión, estos espacios – y, por lo tanto, lo que las personas puedan decir y hacer en línea – son gobernados casi por completo por un pequeño número de empresas tecnológicas. Sus políticas de moderación de contenidos dictan lo que se puede o no ver, decir o hacer en dichas plataformas, y las decisiones se toman cada vez más en base a algoritmos e inteligencia artificial, a la vez que dirigen qué información las

personas ven en línea. En su informe del año 2018 frente a la Asamblea General de la ONU, el Relator Especial de la ONU sobre el derecho a la libertad de opinión y expresión destacó que la manera en que el uso de algoritmos e inteligencia artificial filtra y personaliza el contenido que las personas acceden en línea debilita la capacidad de los titulares de derechos a formar sus propias opiniones en base a una diversidad de ideas provenientes distintas vertientes ideológicas y políticas.[40]

Se han planteado inquietudes relativas a la libertad de expresión en el contexto de legislaciones y propuestas legislativas elaboradas por gobiernos y organismos reguladores que buscan abordar ciertas formas de contenido, expresión y comportamiento en línea. Esta tendencia regulatoria se basa en la evidencia de que las plataformas en línea se han utilizado para difundir desinformación y propaganda política,[41] contenido violento y abusos en contra de las mujeres,[42] así como también incitación al odio y a la violencia contra las minorías.[43] Incidentes violentos tales como el atentado de Christchurch de 2019 en Nueva Zelanda, el incremento de ataques por parte de supremacistas blancos a nivel mundial y la campaña de limpieza étnica en contra de la minoría musulmana rohingya en Myanmar,[44] han puesto en evidencia una relación preocupante entre la proliferación de contenido en línea marcada por el odio y la perpetración de actos violentos fuera de línea.

Otro riesgo crítico hacia la libertad de expresión en línea se origina por las restricciones al acceso a Internet – y, por ende, a las plataformas que allí funcionan – impuestas por gobiernos que buscan controlar los flujos de información. Tan solo en el año 2018, 196 interrupciones del servicio de internet en 25 países bloquearon el acceso a la información de los usuarios, lo que incrementó a 213 interrupciones del servicio en 33 países durante el año 2019.[45] Los grupos en riesgo de discriminación son especialmente vulnerables a aquellas restricciones de acceso arbitrarias, medidas que, a menudo, son tomadas por los gobiernos al margen de la ley con el objetivo de silenciar voces disidentes.[46] Interrupciones extensas del servicio son ejecutadas frecuentemente en regiones donde grupos etnolingüísticos o religiosos marginados constituyen un porcentaje considerable de la población.[47] Investigaciones recientes reconocen la discriminación digital en el acceso a las tecnologías de la comunicación como una tendencia a nivel mundial que afecta fuertemente a grupos étnicos privados de sus derechos.[48]

El Consejo de Derechos Humanos de la ONU condena las medidas que buscan prevenir o interrumpir de forma intencional el acceso o la difusión de información en línea, considerándolas como violaciones al derecho internacional de los derechos humanos, y ha llamado a todos los Estados a evitar y cesar dichas medidas.[49] Dichas interrupciones del servicio de Internet y otras técnicas de control sobre el acceso al mundo digital se basan en la participación de aquellas compañías – a través de medios coercitivos o no – que

operan y mantienen la infraestructura de Internet, incluyendo las telecomunicaciones y los proveedores de servicios de Internet, puntos de intercambio de Internet y redes de distribución de contenido.[50]

Los riesgos a la libertad de expresión también pueden originarse desde las decisiones de los organismos de normalización de Internet. Por ejemplo, en 2019 una coalición de organizaciones de defensa de los derechos digitales pidió públicamente que la Corporación para la Asignación de Números y Nombres en Internet (ICANN, por sus siglas en inglés) prevenga la venta del dominio de alto nivel ".org" – usado principalmente por organizaciones benéficas y otras sin ánimo de lucro – a fondos de capital privado. La coalición argumentó que la gestión de ese dominio por parte de una organización con ánimo de lucro podría tener implicaciones financieras y políticas que exacerbarían el espacio cada vez más reducido para la sociedad civil en todo el mundo.[51]

Por último, la sociedad civil y los defensores de los derechos digitales han señalado que el cumplimiento de la libertad de expresión en línea exige que los actores estatales y privados tomen medidas para proporcionar el acceso a una conexión de Internet asequible y significativa. En un contexto donde aproximadamente el 40 % de la población global no es usuaria activa de Internet,[52] terminar con la brecha digital entre y dentro de los países se ha convertido en una cuestión de derechos humanos crucial. Por otra parte, el Relator Especial de la ONU

© John Schnobrich

sobre la promoción y la protección del derecho a la libertad de opinión y expresión enfatizó que la calidad y el tipo de acceso a Internet puede también tener impactos negativos sobre el derecho a la libertad de expresión. Por ejemplo, las amenazas al principio de la "neutralidad de la red" y los planes de tasa cero podrían restringir y limitar de forma indebida el tipo de contenido e información que ciertos usuarios pueden acceder en línea.[53]

Marcos e iniciativas

En este contexto, los Estados están adoptando legislación que exige o alienta a las empresas tecnológicas a identificar y eliminar las diferentes formas de contenido "dañino" generado y colgado por los usuarios, incluyendo el establecimiento de sistemas de responsabilidad legal de los intermediarios. Por ejemplo, en 2018 Alemania adoptó una ley llamada Ley de Aplicación de Redes (NetzDG), la cual exige a las empresas tecnológicas que eliminen contenido que sea "obviamente ilegal", como incitaciones al odio u otras publicaciones en un plazo de 24 horas a partir de la recepción de una queja. Además, las compañías enfrentan multas de hasta 50 millones de euros en caso de incumplimiento de la ley. En abril de 2019, Australia modificó su Código Penal para tipificar como delito la publicación de "material aberrante y violento" y para exigir a las empresas tecnológicas que eliminen el contenido violento en línea con celeridad. Las sanciones por el no cumplimiento son altas: las empresas pueden ser multadas hasta por el 10% de sus ganancias anuales y, además, los ejecutivos de las empresas arriesgan condenas privativas de libertad.

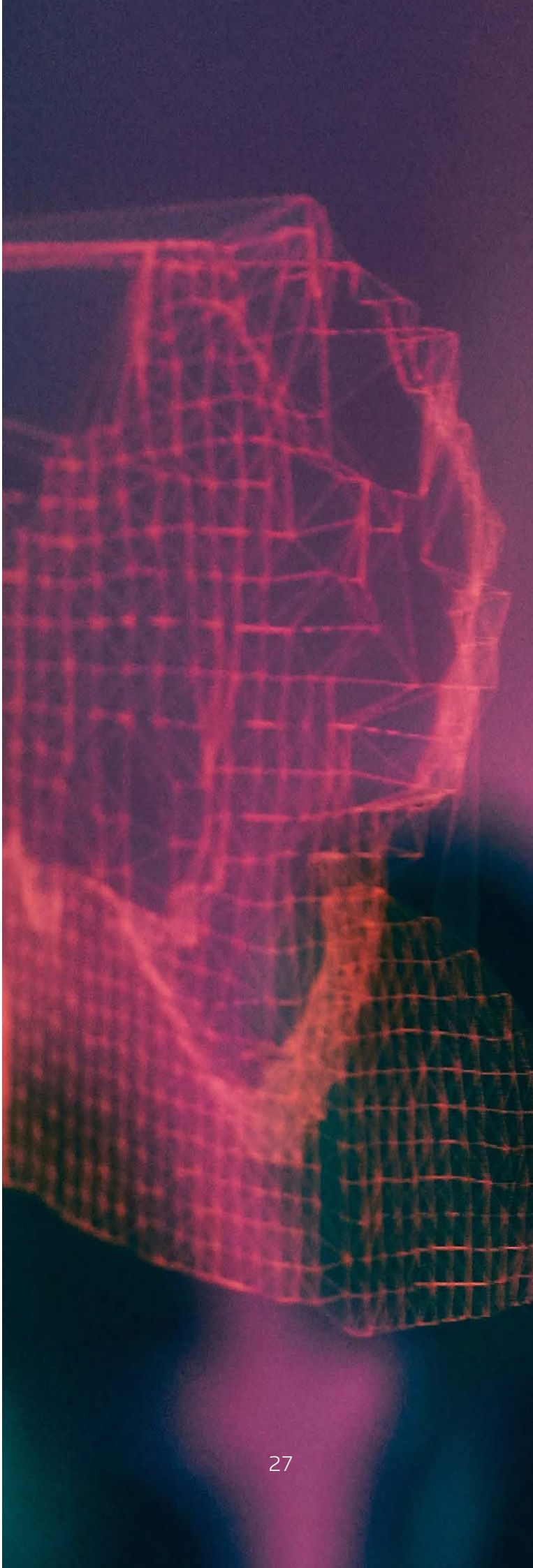
Asimismo, otras jurisdicciones han considerado el desarrollo de regulaciones similares. En efecto, en 2019 el Reino Unido reveló un plan para un nuevo régimen normativo que podría establecer un "deber de diligencia" de parte de las empresas tecnológicas para proteger la seguridad de sus usuarios, así como un organismo regulador independiente con el fin de garantizar el cumplimiento.[54] A nivel de la UE, el Parlamento Europeo ha respaldado proyectos que podrían exigir a las plataformas en línea eliminar el contenido terrorista dentro de una hora después de la notificación de su publicación por parte de autoridades nacionales. Un estudio realizado por la Freedom House descubrió que, en el año 2017, al menos 17 países aprobaron o propusieron leyes que podrían restringir las plataformas de medios en línea en nombre de la lucha contra las "fake news" y la manipulación en línea.[55]

Mientras los gobiernos que proponen leyes como las mencionadas, por lo general, indican que cualquier restricción sobre la libertad de expresión sería justificada, diversos expertos en materias de derechos humanos han cuestionado la certeza jurídica, la proporcionalidad y la necesidad de estas leyes y propuestas, dadas sus definiciones vagas, altas penas y plazos breves. Se han planteado numerosas inquietudes con

relación a esas leyes, y se ha señalado que podrían incentivar la eliminación excesiva de contenido que se ajusta a la ley, así como formas de expresión legítimas.

Más allá de cumplir con leyes nacionales, las empresas tecnológicas aplican sus propias reglas (las que son descritas como términos y condiciones, normas comunitarias, entre otras) sobre las modalidades aceptables y los tipos de expresión y comportamiento en sus plataformas. Se ha sostenido que la aplicación arbitraria de dichas reglas y su limitada alineación con las normas de derechos humanos han restringido de manera desproporcionada y discriminatoria la libertad de expresión.[56]

Organizaciones de la sociedad civil han señalado varias instancias de supresión de la libertad de expresión en plataformas de medios sociales, incluyendo activismo LGBTI, información sobre limpieza étnica y denuncias sobre racismo y estructuras de poder.[57] Un análisis de los términos de servicio de Facebook y Twitter concluyó que sus definiciones y prácticas necesitan alinearse con las normas internacionales sobre libertad de expresión.[58] A su vez, la identificación de contenido inapropiado a través del uso de algoritmos ha sido criticada por fallar al tratar de interpretar de manera correcta mensajes provenientes de culturas y contextos específicos. Asimismo, el Relator Especial de la ONU sobre el derecho a la libertad de opinión y expresión ha señalado que existe



© Ashwin Vaswani

un alto riesgo de que los sistemas de moderación de contenido que utilicen inteligencia artificial eliminen contenido de acuerdo con conceptos discriminatorios sesgados y que, como resultado, los grupos vulnerables serán probablemente los más perjudicados. [59]

Numerosos expertos y defensores han propuesto principios de derechos humanos para la moderación de contenido con el fin de abordar el excesivo e inapropiado cierre de cuentas y eliminación de contenido. Por ejemplo, los Principios de Santa Clara sobre la transparencia y la responsabilidad en la moderación de contenidos consisten en un conjunto de normas de referencia que tienen como objetivo asegurar que la moderación de contenidos sigua un debido proceso, tales como notificar y dar pie a una apelación oportuna a cada usuario cuyo contenido sea retirado o cuya cuenta sea suspendida.[60] Asimismo, una coalición de expertos de la sociedad civil desarrollaron los Principios de Manila sobre responsabilidad legal de los intermediarios como parte un esfuerzo más amplio por incorporar los principios de derechos humanos en marcos regulatorios de contenido en línea.[61]

En el informe de 2018 frente al Consejo de Derechos Humanos, el Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y expresión propuso un conjunto de principios de derechos humanos para orientar la moderación del contenido en línea,[62] y destacó entre otras cosas, que cuando las empresas elaboren o modifiquen políticas o productos, deberían tratar de conocer cuáles son las preocupaciones de las comunidades que históricamente se han enfrentado al peligro de la censura y la discriminación. [63]

Por otra parte, nuevos modelos de gobernanza sobre moderación de contenidos han aparecido como respuesta a los llamados por más responsabilidad y transparencia en las plataformas sociales. En 2019, la organización de la sociedad civil Article 19 lanzó una consulta pública sobre la creación de Consejos de Redes Sociales, foros para múltiples partes interesadas cuya finalidad sería abordar las cuestiones sobre moderación de contenidos en plataformas de medios sociales sobre la base de las normas internacionales de derechos humanos.[64] En 2020, Facebook lanzó un consejo de supervisión independiente cuya tarea es revisar las apelaciones contra las decisiones de la compañía relativas a la moderación de contenidos.[65]

Además de un enfoque basado en reglas para la moderación de contenidos, organismos públicos y empresas tecnológicas han hecho alianzas para elaborar programas sociales que aborden la manipulación y la desinformación en línea. Por ejemplo, en Italia, los responsables de la formulación de políticas públicas han cooperado con periodistas y firmas tecnológicas para elaborar y poner a prueba un programa a nivel nacional sobre identificación de manipulación en línea, incluyendo las “fake news” y teorías de la conspiración.[66] Por

su parte, Apple lanzó una iniciativa de alfabetización mediática para fomentar el pensamiento crítico y empoderar a los estudiantes para que estén mejor informados. Los Estados Unidos se asoció con diferentes organizaciones sin ánimo de lucro, tales como News Literacy Project y Common Sense, que proporcionan programas de alfabetización mediática independientes y no partidistas.[67] Asimismo, WhatsApp ha trabajado con organizaciones en India para diseñar un programa de alfabetización digital para sus usuarios.[68] Las empresas tecnológicas han hecho alianzas con la sociedad civil con el fin de combatir la desinformación en sus plataformas. La organización argentina Chequeado ejecuta una aplicación de software en alianza con Facebook para hacer coincidir de forma automática reclamos en la red con investigación de verificación de los hechos.[69]

3. EL SECTOR TECNOLÓGICO EN PLANES DE ACCIÓN NACIONALES DE EMPRESAS Y DERECHOS HUMANOS

Esta Sección se desarrolla en base a las orientaciones sobre el ciclo de vida de un PAN que se encuentran en el Kit de herramientas del DIHR-ICAR, y determina la forma en que los Estados pueden asegurar que las especificaciones relacionadas al sector tecnológico sean consideradas en el proceso y contenido de un PAN.

3.1. MAPEO Y PARTICIPACIÓN DE LAS PARTES INTERESADAS

Tal como señala el Kit de herramientas del DIHR-ICAR, es esencial que todos los grupos de interés (partes interesadas) relevantes estén mapeados y participen durante la elaboración de un PAN. Además, su participación debería darse de manera abierta, inclusiva y transparente. Los organismos estatales que tengan un mandato pertinente a las operaciones del sector tecnológico deberían ser incluidas dentro del diseño e implementación del proceso, incluyendo, a través de la asignación de recursos para el desarrollo de capacidades, participación en la recopilación de datos y consultas públicas y a expertos. Es crucial que el mapeo de las partes interesadas incluya a personas y grupos cuyos derechos a la privacidad, la libertad de expresión y la no discriminación se encuentren más amenazados, tales como defensores de los derechos humanos, mujeres y niñas, minorías étnicas o religiosas, o personas discriminadas debido a su orientación sexual e identidad de género. Se deben elaborar estrategias específicas para la participación de estas personas y grupos, con el fin de asegurar que sus

derechos sean protegidos y sus voces escuchadas durante el proceso.

Existen numerosas categorías generales de partes interesadas que debieran ser consideradas durante el proceso de elaboración de un PAN, independientemente del sector en el que se desempeña la empresa o del ámbito político. Con el objetivo de ayudar a los actores estatales que utilicen el Kit de herramientas del DIHR-ICAR, las categorías incluidas en él se enumeran a continuación y, en su caso, las partes interesadas específicas que debieran ser consideradas en cuanto al sector tecnológico.

Categoría de las partes interesadas	Categoría de las partes interesadas Partes interesadas específicas para el sector tecnológico
El gobierno ejecutivo, incluidos todos los departamentos gubernamentales, agencias, oficinas y empresas estatales pertinentes, así como la policía y otras agencias encargadas de hacer cumplir la ley	• Ministerios de Comunicaciones y/o de las tecnologías de la información • Ministerios de Justicia • Oficinas enfocadas en la tecnología dentro de otros ministerios, por ejemplo, “embajador tecnológico” en el Ministerio de Relaciones Exteriores o una “oficina para la tecnología y la innovación” en un Ministerio de Economía • Policía y fuerzas del orden con responsabilidad por el cibercrimen • Autoridades responsables de los contratos públicos, así como compradores públicos • Organismos reguladores cuyos mandatos incluyan la tecnología de Internet y digital (Véase el Cuadro 5) • Organismos reguladores cuyos mandatos incluyan organizaciones de medios tradicionales y nuevos

El poder judicial y los tribunales administrativos, los mecanismos alternativos de resolución de conflictos y los actores informales de justicia	• Defensoría del Pueblo para la transformación digital (o similar)' • Defensoría del Pueblo para la Igualdad (o similar) • Asociaciones de abogados
El Parlamento, incluidas las comisiones pertinentes	• Comisiones parlamentarias cuyo mandato cubra las comunicaciones y/o tecnologías de la información • Comisiones parlamentarias cuyo mandato cubra el acceso a la justicia, el crimen y/o el cibercrimen • Comisiones parlamentarias cuyo mandato cubra la
Las empresas, incluidos los sectores industriales importantes, las asociaciones empresariales, pequeñas y medianas empresas (pymes), los autónomos, los comerciantes individuales, las cooperativas, las organizaciones sin ánimo de lucro y los agentes del sector informal	• Organismos de la industria del sector tecnológico • Empresas tecnológicas que operen o que estén domiciliadas en el país
Los sindicatos y otras asociaciones de representantes de los trabajadores	• Sindicatos a nivel nacional e industrial que trabajen sobre la cuestión de la recopilación de datos de los trabajadores, la supresión de las voces de los trabajadores a través del monitoreo de los medios sociales, la no discriminación, etc.

Los representantes de grupos o comunidades de titulares de derechos y defensores de los derechos humanos, localizados dentro y fuera de la jurisdicción territorial del Estado, que puedan verse potencialmente afectados por la conducta de empresas basadas en o controladas por el Estado	• Representantes de los titulares de derechos que puedan ser especialmente marginados, por ejemplo, mujeres y niñas, personas que pertenezcan a la comunidad LGBTI, minorías étnicas y religiosas etc. • Defensorías para la igualdad que se enfoquen en privacidad, libertad de expresión y/o Internet y tecnología digital (incluyendo organizaciones de defensa de los derechos digitales) • Defensorías para la igualdad (organizaciones de la sociedad civil, abogados y aquellos que trabajen en cuestiones de igualdad y no discriminación) • Organizaciones de consumidores que representen los derechos de los consumidores/usuarios cuyos derechos puedan ser violados • Organizaciones de libertad de prensa
Las INDH, las instituciones de Defensorías del Pueblo, los organismos estatutarios de igualdad, y otros mecanismos de rendición de cuentas con un mandato de derechos humanos	• Instituciones nacionales de derechos humanos (véase el Cuadro 6) • Autoridades de protección de datos • Organismos nacionales que trabajen en materia de igualdad
Organizaciones de la Sociedad civil con mandatos que aborden las cuestiones relevantes	• Defensorías para la igualdad que se enfoquen en privacidad, libertad de expresión y/o Internet y tecnología digital (incluyendo organizaciones de defensa de los derechos digitales)

	• Defensorías para la igualdad (organizaciones de la sociedad civil, abogados y aquellos que trabajen en cuestiones de igualdad y no discriminación) • En caso de que no existan dichas organizaciones dentro del Estado, se pueden involucrar organizaciones internacionales, tales como Global Partners Digital, Equal Rights Trust, Access Now, Association for Progressive Communications, Article 19 y Privacy International
Los medios, incluidas las fuentes de noticias generales y especializadas	• Compañías de medios en línea • Foros en línea
La academia, incluyendo los institutos de investigación, los expertos individuales y las instituciones educativas relevantes, tales como las escuelas de negocios	• Instituciones académicas y de investigación que se especialicen en Internet y tecnología digital
Los actores internacionales y regionales, incluidos los organismos pertinentes de las Naciones Unidas, el Banco Mundial, los bancos regionales de desarrollo y la OCDE	• Unión Internacional de Telecomunicaciones • Comisión de Ciencia y Tecnología para el Desarrollo de la ONU • UNICEF, Equipo de Derechos del Niño y Empresas • Oficina del Alto Comisionado para los Derechos Humanos (ACNUDH) • Consejo de Europa, Departamento contra la Discriminación

Organismos reguladores

En cuanto a la regulación del sector tecnológico (y la tecnología en general), cada Estado utiliza su propio método. Algunos de ellos otorgan nuevas funciones y poderes a los organismos reguladores ya existentes, como, por ejemplo, a las autoridades de protección de datos. Otros han establecido nuevos organismos reguladores cuyos mandatos hacen referencia a diferentes aspectos de la Internet o la tecnología.

Australia: En 2015 Australia creó el Children's eSafety Commissioner, cuyo mandato es proteger la seguridad de los niños y las niñas en línea. Desde ese momento, el mandato del organismo (ahora el eSafety Commissioner) se amplió con el fin de tomar medidas de prevención contra el abuso basado en imágenes y otras formas de contenido prohibido.

Dinamarca: El Data Ethics Council de Dinamarca está conformado por miembros que representan una amplia gama de competencias, tanto del sector público como del privado. El organismo proporciona asesoría y recomendaciones al gobierno danés, al Parlamento y a las autoridades sobre cuestiones relativas a la ética del uso de datos y de las nuevas tecnologías, y para respaldar una cultura de utilización de datos responsable por parte de las empresas y el público.

Reino Unido: El Centre for Data Ethics and Innovation se estableció en el año 2018 con el mandato de analizar y anticipar las oportunidades y riesgos planteados por la tecnología basada en datos (con especial enfoque en la inteligencia artificial) y para promover el asesoramiento práctico y basado en datos empíricos para abordarlos.

Instituciones nacionales de derechos humanos

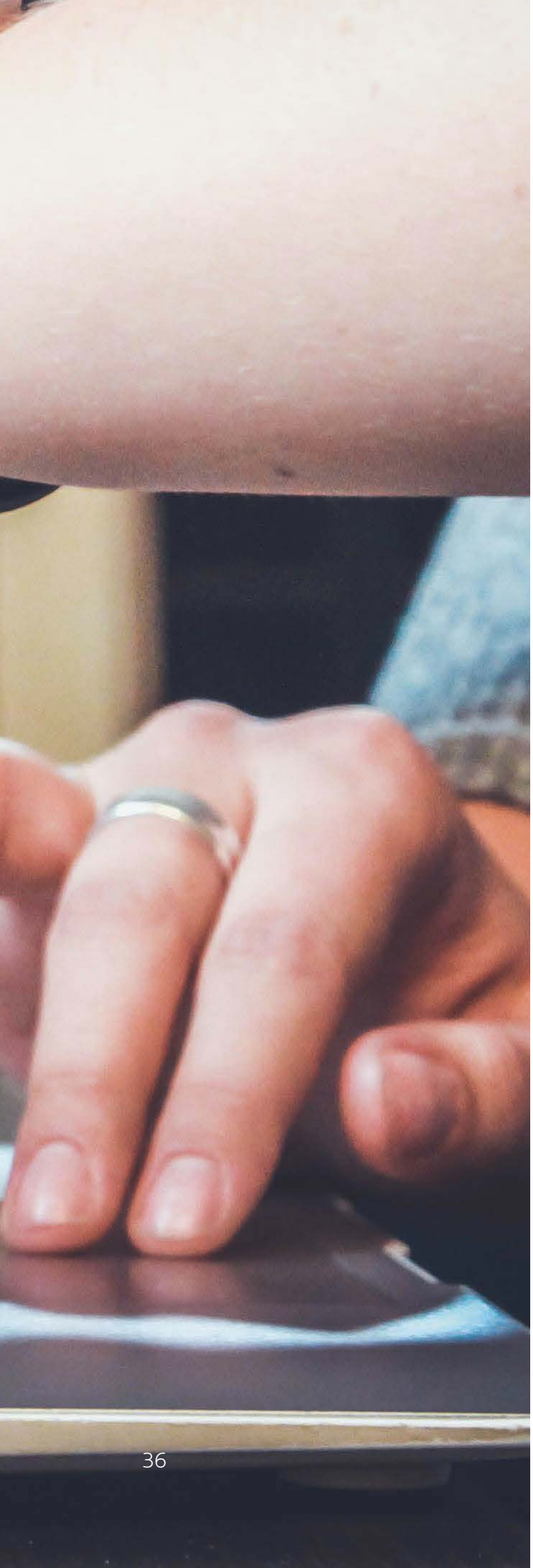
Las instituciones nacionales de derechos humanos (INDH) se están interesando cada vez más en la tecnología y en los impactos que ésta tiene sobre los derechos humanos, en ocasiones como parte de su trabajo en general sobre empresas y derechos humanos. En este sentido, deben proporcionar una perspectiva específica sobre cómo los derechos humanos, tales como la privacidad y la libertad de expresión, pueden verse afectados por el sector tecnológico durante la elaboración de un PAN.

Australia: En 2018, la Comisión Australiana de Derechos Humanos (AHRC, por sus siglas en inglés) lanzó un proyecto sobre la relación existente entre los derechos humanos y la tecnología. Con el asesoramiento proporcionado por un grupo experto de consulta integrado por representantes de la academia, del área de los negocios

y del Estado, el proyecto explora cuestiones de derechos humanos vinculadas a la inteligencia artificial, sesgos, big data, tecnología inclusiva y a la intersección entre tecnología, libertad de expresión y democracia. La AHRC tiene planes de formular recomendaciones para asegurar que los derechos humanos sean priorizados en el diseño y la gobernanza de tecnologías emergentes en 2020.

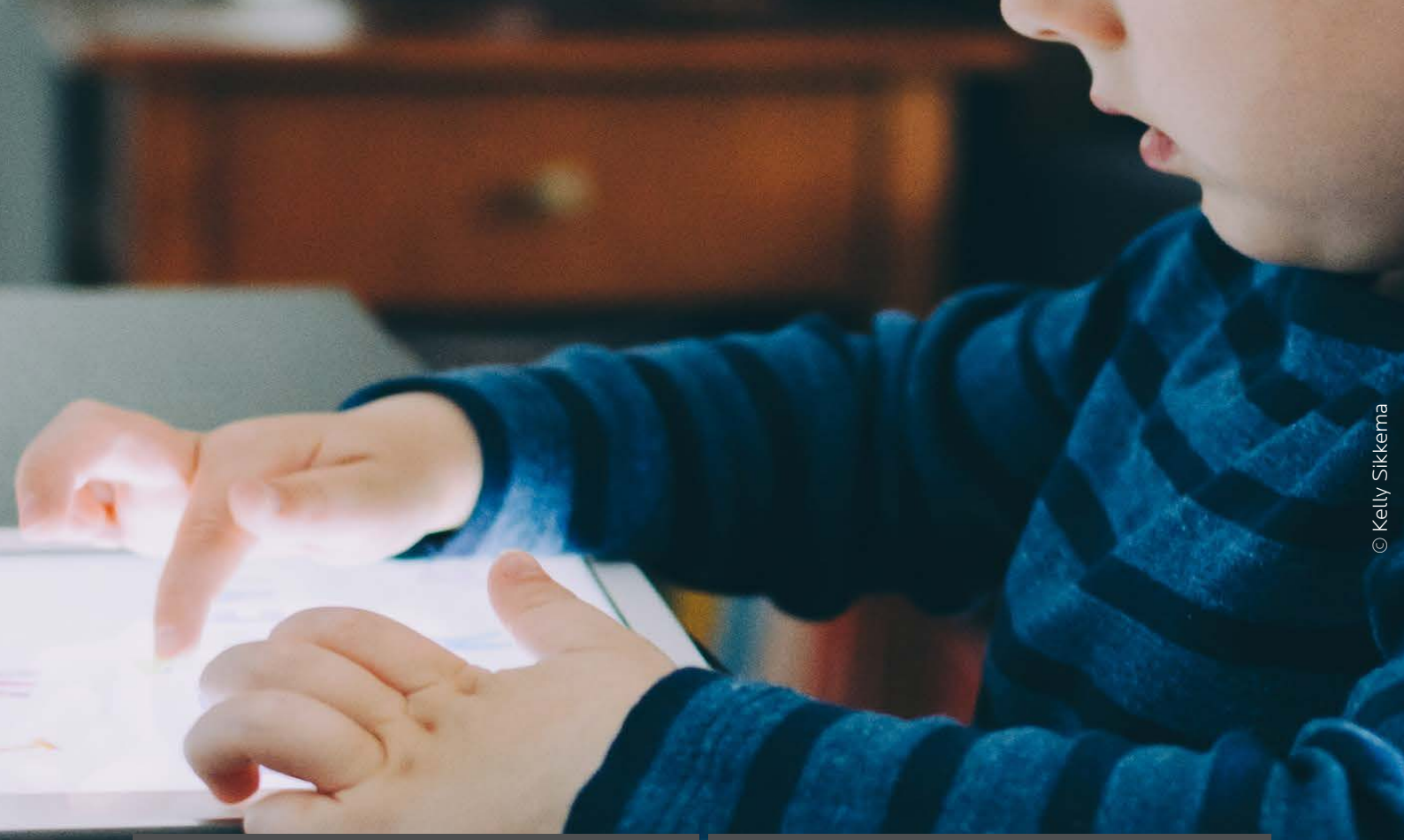
Dinamarca: El Instituto Danés de Derechos Humanos ha realizado investigación específica en materia de tecnología y sus impactos sobre los derechos humanos desde el año 2003. Ha contribuido al establecimiento de normas en esta área en la ONU, la UE y en el Consejo de Europa. El Instituto trabaja con empresas tecnológicas y, actualmente, se encuentra en proceso de elaboración de directrices sobre cómo llevar a cabo evaluaciones de impacto en derechos humanos de actividades de empresas digitales.

Kenia: En febrero de 2019, la Comisión Nacional Derechos Humanos de Kenia (KNCHR, por sus siglas en inglés), junto a la Comisión de Derechos Humanos de Kenia y el Foro de Derechos Nubio, presentó una solicitud ante el Tribunal Superior de Nairobi para evitar la implementación de un sistema de registro digital nacional de identificación obligatorio – el Sistema Nacional Integrado de Gestión de la Identidad (NIIMS, por sus siglas en inglés). La KNCHR apoyó a los otros solicitantes argumentando, entre otras cosas, que el NIIMS viola el derecho a la privacidad, dado que no garantiza protecciones adecuadas, y los derechos a la igualdad y la no discriminación de la comunidad nubia y otros grupos marginados podrían enfrentar aún más exclusión. El 30 de enero de 2020 el Tribunal Superior determinó que el gobierno de Kenia debería interrumpir la implementación del sistema hasta que exista un marco jurídico apropiado y exhaustivo para ello. El fallo reconoció la importancia de tener un marco de protección de datos y un marco jurídico claro que aborde la posibilidad de exclusión.



3.2. GRUPOS EN RIESGO

Al igual que en otros sectores empresariales y áreas de políticas, es importante considerar y responder a las necesidades y las experiencias de diversos grupos, particularmente de los grupos en riesgo, al mapear (y al participar con) las partes interesadas.[70] En cuanto al sector tecnológico, existen titulares de derechos y grupos que se encuentran especialmente en riesgo de que sus derechos humanos sean violados, por lo tanto el Estado debiera identificar a aquellas personas, organismos y organizaciones que de forma legítima representen los intereses de los grupos mencionados, asegurando que su participación no resultará en represalias o acoso de ninguna forma. La tabla a continuación incluye algunos ejemplos de impactos negativos y discriminatorios en los derechos a la privacidad y la libertad de expresión sobre personas con ciertas características. Es una lista que no tiene carácter exhaustivo y los Estados debieran asegurar que todos los grupos que podrían verse afectados de forma desproporcionada por las políticas relativas al sector tecnológico sean motivadas y habilitadas para participar en las consultas.



© Kelly Sikkema

Características / Grupo	Algunos ejemplos de impactos negativos y discriminatorios en los derechos a la privacidad y la libertad de expresión
EDAD / NIÑOS Y NIÑAS	
Los niños y las niñas se encuentran en riesgo de manera desproporcionada frente a la recopilación de datos excesiva, la manipulación en línea y el abuso, dadas sus capacidades cognitivas, sociales y emocionales en desarrollo. Las empresas recopilan datos sobre niños y niñas desde el momento en que nacen sin su conocimiento y sin estar conscientes de esto a través de información compartida por sus padres y debido al uso de dispositivos de control parental. La publicidad dirigida y los modelos de motores de búsqueda pueden ser perjudiciales en el desarrollo	• La Comisión Federal de Comercio de los Estados Unidos ha impuesto numerosas multas a empresas tecnológicas por recopilar datos personales de niños y niñas sin el consentimiento de sus padres. • Según Human Rights Watch, la ley rusa sobre “propaganda gay” de 2013 prohíbe la “promoción entre menores de las relaciones sexuales no tradicionales”, lo que ha tenido un impacto negativo sobre los jóvenes de la comunidad LGBTI que intenten acceder a sitios web educacionales y servicios de apoyo en línea.

de los niños y las niñas, al influenciar sus preferencias como consumidores y su habilidad de desarrollar opiniones autónomas. La creciente presencia de los niños y las niñas en los medios sociales y otras plataformas digitales ha incrementado los riesgos de abuso sexual, hostigamiento y ciberacoso.

• Según un reciente estudio sobre la distribución de capturas de abuso sexual infantil transmitido en vivo, el 98% de las imágenes mostraban niños y niñas de al menos 13 años o menores, y el 96% de ellas mostraba a niñas.

• Las escuelas en los Estados Unidos han contratado empresas de monitoreo de medios sociales con el fin de prevenir la violencia y los tiroteos escolares. Sin embargo, los programas de monitoreo han sido cuestionados por la interferencia desproporcionada en el ejercicio de la libertad de expresión en línea de los y las adolescentes.

GÉNERO/MUJERES

La discriminación que enfrentan las mujeres fuera de línea ha permeado los espacios digitales. En 2018, el Consejo de Derechos Humanos de la ONU adoptó una resolución que reconoce la cuestión de la discriminación y la violencia en contra de las mujeres en los contextos digitales. Nueva terminología ha sido introducida para entender los nuevos tipos emergentes de violencia en línea, incluyendo los conceptos de "doxing", "sextorsión", "trolling", acoso y asecho en línea y "pornovenganza" (la distribución de contenidos íntimos sin consentimiento). La publicación sin consentimiento de imágenes íntimas representa violencia de género y una violación a los derechos de privacidad de

• Un estudio realizado en 2018 por Amnistía Internacional detectó que las mujeres son más propensas a ser acosadas y abusadas en Twitter, incluso a través de violaciones de privacidad como "doxing" o la divulgación de imágenes íntimas o de contenido sexual sin consentimiento. El acoso en línea resulta, a menudo, en que las mujeres autocensuran sus publicaciones y dejan Twitter. Según el informe, Twitter ha investigado y respondido a las denuncias de violencia y abuso de manera inadecuada.

• En 2019, una mujer miembro de la Cámara de Representantes de los Estados Unidos renunció a su cargo luego

mujeres y niñas. Las amenazas y el abuso en línea impiden que las mujeres ejerzan su derecho a la libertad de expresión, incluso a través de su salida de plataformas digitales, debates y funciones públicos. Las defensoras de los derechos humanos, las mujeres dedicadas a la política y las periodistas se encuentran en mayor riesgo de sufrir violencia en línea.

Por otra parte, la discriminación, la desigualdad y los estereotipos en línea resultan en una división digital de género donde es menos probable que

las mujeres y las niñas utilicen Internet y se beneficien de las oportunidades de conexión financieras, educacionales, y sociales en línea que los hombres.

de que medios informativos divulgasen en línea fotografías íntimas sin su consentimiento.

• Una encuesta realizada en 2018 por la Unión Interparlamentaria descubrió que un número significativo de mujeres miembros del Parlamento ha sufrido experiencias de contenido abusivo, de carácter sexual y violento en redes sociales.

• En el año 2016, Al Jazeera informó sobre la existencia de un mercado de venta de videos de violaciones en el Estado de Uttar Pradesh, India.

• Según un estudio realizado en 2019 con mujeres periodistas en Pakistán, éstas denuncian que la violencia en línea ha tenido un impacto importante en su salud mental y que se autocensuran para contrarrestar la violencia en línea.

• Activistas han expresado la preocupación de que los datos personales recolectados a través de dispositivos inteligentes en el hogar y de tecnologías digitales puedan ser utilizados para controlar e intimidar a las víctimas de violencia doméstica.

• Según la Unión Internacional de Telecomunicaciones, en 2017, la proporción de mujeres que utilizaba Internet era 12% menor que la proporción de hombres en el mundo entero. La brecha se expande en África, donde la proporción de mujeres que utiliza Internet era 25% menor que la proporción de hombres.

© Gayatri Malhotra

DEFENSORES DE LOS DERECHOS HUMANOS

Los defensores de los derechos humanos en todo el mundo dependen de la tecnología para organizarse, movilizarse y defender los derechos humanos. Si bien su presencia digital ha aumentado, también lo ha hecho su susceptibilidad a la vigilancia y control en línea a través de productos espía, lo que ha traído consigo implicancias adversas contra su seguridad y privacidad. De manera creciente, gobiernos han ordenado interrupciones del servicio de Internet para silenciar a los defensores de los derechos humanos.

• Según Amnistía Internacional, la empresa israelí NSO Group desarrolló tecnología de programas espías que se utilizaron para silenciar a defensores de los derechos humanos en países como México, Marruecos y Arabia Saudita. En octubre de 2019, WhatsApp demandó a la empresa NSO Group, alegando que ayudó al gobierno a acceder a los dispositivos de aproximadamente 1.400 usuarios, entre los que se encontraban periodistas y disidentes políticos.

• En 2019, un grupo de organizaciones de la sociedad civil expresó su preocupación sobre la tendencia a nivel mundial de perseguir a los defensores de derechos digitales.

• Según Human Rights Watch, el corte de Internet impuesto por el Consejo Militar de Transición de Sudán en 2019 impidió que activistas divulgaran información crítica en el contexto de una crisis política.

RAZA, ETNIA Y RELIGIÓN

La discriminación sobre la base de la raza, etnia y religión se ha extendido al ámbito en línea, a través de la vigilancia digital, las restricciones ilegítimas sobre la libertad de expresión, así como también a través de una inadecuada moderación del contenido que induce a la violencia.

• Una fuga de datos en 2019 reveló que China hacía seguimiento de localización a casi 2,6 millones de personas a través de la empresa de reconocimiento facial llamada SenseNets en la región de Xinjiang, donde habitan ciudadanos de la etnia uigur y otras minorías musulmanas.

• Vox informó sobre dos estudios científicos que demostraron que los modelos de inteligencia artificial utilizados por medios sociales son 1,5 veces más proclives a marcar tuits escritos por afroestadounidenses como "ofensivos" en comparación con otros tuits.

• Un estudio realizado en 2019 por la Universidad de Cardiff dejó al descubierto una correlación entre los discursos de odio en Twitter que se refieren a raza y religión y el agravamiento de las ofensas raciales y religiosas que sucedieron fuera de línea durante el mismo período.

• En 2020, como parte de las protestas del movimiento Black Lives Matter a nivel mundial, se prestó más atención a las políticas de moderación de contenidos de los principales medios sociales cuando existieron discursos de odio e incitación a la violencia. Asimismo, se dio mayor énfasis a la necesidad de mayor acción para abordar la manera en que las personas utilizan las plataformas de medios sociales para violar los derechos humanos.

• En 2019 la Corporación para la Asignación de Números y Nombres

en Internet (ICANN, por sus siglas en inglés) otorgó el derecho exclusivo para administrar el dominio de nivel superior ".amazon" a la compañía Amazon. Algunos expertos en derechos humanos sostuvieron que esta decisión privaría a los pueblos indígenas de la zona del Amazonas de oportunidades de desarrollo económico y que bajo el derecho internacional de derechos humanos la compañía Amazon era responsable de asegurar que los pueblos indígenas fueran consultados antes de seguir con la solicitud para registrar el dominio.

• En febrero de 2020, el gobierno de Myanmar reinstauró un corte del tráfico de Internet móvil en cinco municipios en los Estados de Rakhine y Chin. Lo que se sumó a cuatro municipios del Estado de Rakhine que han sido privados del servicio desde junio de 2019, provocando una restricción de información que afecta aproximadamente a un millón de personas, la mayoría pertenecientes a la minoría étnica musulmana rohingya. Bloquear su habilidad de comunicarse dificulta la obtención de ayuda en tiempos de conflicto y que las agencias humanitarias proporcionen asistencia.

ORIGEN NACIONAL O SOCIAL / TRABAJADORES MIGRANTES

De manera creciente, los trabajadores migrantes han sido sujetos de impactos sobre su derecho a la privacidad por parte de empresas tecnológicas, dada su posición vulnerable en la sociedad, donde no tienen protección.

• Una investigación realizada por la BBC descubrió que cientos de trabajadores domésticos en Kuwait están siendo comprados y vendidos de forma ilegal a través de Instagram y sus datos personales, tales como imágenes y raza, están siendo puestos a disposición de potenciales "compradores".

© Markus Spiske

ORIENTACIÓN SEXUAL E IDENTIDAD DE GÉNERO

Las personas que pertenecen a la comunidad LGBTI se enfrentan a graves riesgos de ser víctimas de discursos de odio y violencia en línea, así como a impactos desproporcionados sobre su derecho a la privacidad y restricciones en su derecho a la libertad de expresión.

- El Relator Especial de la ONU sobre el derecho a la libertad de opinión y expresión señaló que las "plataformas habrían reprimido el activismo en favor de las personas lesbianas, gais, bisexuales, transgénero y asexuadas" y ha supuesto el "bloqueo de las cuentas de usuarios y activistas en favor de los derechos de las personas lesbianas, gais, bisexuales, transexuales, artistas travestidos y de las cuentas de usuarios con nombre que no son ingleses o que son poco convencionales".
- Las comunidades LGBTI han alegado que el algoritmo de YouTube bloquea o elimina videos que incluyen contenido LGBTI, al aplicar automáticamente la restricción de edad y al "desmonetizar" los videos, lo que significa que niegan las ganancias de los productores.

3.3. REALIZAR UNA EVALUACIÓN NACIONAL DE LÍNEA DE BASE

Una etapa importante dentro del ciclo de vida de un PAN es llevar a cabo una Evaluación Nacional de Línea de Base (ENLB).[71] Tal como el Kit de herramientas de DIHR-ICAR establece, "una ENLB sobre empresas y derechos humanos tiene el objetivo principal de evaluar el nivel actual de implementación de los Principios Rectores en un Estado determinado. Reúne un análisis de las lagunas legales y políticas en la implementación de los Principios Rectores con una visión general de los impactos adversos de las empresas sobre los derechos humanos, para identificar los asuntos más relevantes de derechos humanos en un contexto dado. De esta manera, sirve para informar la formulación y la priorización de acciones en un PAN".

La 'Plantilla para una Evaluación Nacional de Línea de Base (ENLB) y el sector tecnológico' debería ser utilizada para determinar de qué manera los derechos a la privacidad, la libertad de expresión y la igualdad y la no discriminación de aquellos afectados por el sector tecnológico están siendo, a su vez, protegidos como parte del marco político y legal sobre empresas y derechos humanos de los Estados. Está diseñada para ser utilizada en conjunto con la plantilla de ENLB completa que se encuentra en el Kit de herramientas de DIHR-ICAR.

Al realizar una ENLB y utilizarla como una herramienta para elaborar un PAN, los Estados deberían analizar y evaluar la toma de medidas específicas que garanticen tanto la protección por parte del Estado como el respeto de las empresas por los derechos a la privacidad, la libertad de expresión y la igualdad y la no discriminación, así como una reparación efectiva en caso de que se hayan violado dichos derechos.

La plantilla a continuación contiene las preguntas mínimas relativas a la protección y el respeto hacia los derechos a la privacidad, la libertad de expresión y la igualdad y la no discriminación que los Estados deberían considerar cuando se encuentren en proceso de diseño de una ENLB. Las preguntas reflejan las disposiciones de los PRNU sobre el deber de los Estados de proteger contra las violaciones de los derechos humanos (Pilar I), la responsabilidad de las empresas de respetar los derechos humanos (Pilar II) y el acceso a mecanismos de reparación por parte de actores estatales y no estatales (Pilar III). Integrar estas preguntas dentro de una ENLB general permitirá a los responsables de formular políticas públicas obtener información detallada sobre las diferentes formas en que el sector tecnológico se involucra con impactos negativos y discriminatorios en la privacidad y la libertad de expresión. De igual forma, permitirá evaluar su gravedad y decidir si deben ser priorizadas en el PAN y de qué manera debería hacerse.

Los Estados deberían considerar consultar a expertos locales al inicio de una ENLB y también durante el proceso de escritura de su borrador. Entender las operaciones de las empresas tecnológicas y la manera en que pueden afectar los derechos humanos exige conocimiento especializado. Por lo tanto, se recomienda que la organización que esté llevando a cabo la ENLB esté capacitada de forma adecuada para analizar la información relativa a la tecnología, identificar riesgos y entender el complejo ecosistema en que operan las tecnologías.

Como parte de una ENLB, el Estado podría considerar poner en marcha una evaluación de impacto sectorial sobre los derechos humanos.[72] Una evaluación de impacto enfocada en los impactos del sector tecnológico sobre los derechos humanos ayudará a los actores estatales y partes interesadas a contar con un panorama más amplio de los impactos negativos potenciales de las actividades de dicho sector.

Comentario sobre la extraterritorialidad

Si bien es cierto que los PRNU indican que a los Estados no se les exige que regulen las actividades extraterritoriales de las empresas domiciliadas en su territorio y/o jurisdicción, también reconocen que dicha tarea no se les prohíbe, siempre que haya una base jurisdiccional reconocida. Los PRNU reconocen que hay razones políticas de peso para que los Estados sean claros sobre lo que esperan de las empresas en el extranjero. Por otro lado, los Estados no tienen poder ilimitado para promulgar leyes aplicables a las actividades extraterritoriales y deben operar dentro de las limitaciones del derecho y la cortesía internacional.

Si bien esto podría tomarse en consideración en muchos sectores, es particularmente relevante para el sector tecnológico, dado que muchas empresas tecnológicas operan a nivel mundial y ofrecen productos y servicios que son accesibles en todo el mundo y, a menudo, en Estados donde las compañías no tienen presencia física. En vista de la naturaleza intangible de algunas actividades digitales, puede ser difícil identificar dónde ocurren las actividades y qué regulación legal nacional se debería aplicar.

El marco regulatorio que se aplica a compañías en un Estado, en especial en su país de origen, con frecuencia tendrá impactos en otros donde esas compañías operen. Por ejemplo, el RGPD de la UE (véase el Cuadro 4) fija estándares más altos que otros marcos regulatorios nacionales sobre protección de datos. En lugar de tener diferentes políticas de protección de datos para cada Estado, algunas empresas tecnológicas simplemente utilizan las exigencias del RGPD como su política de protección de datos a nivel mundial, lo que, desde una perspectiva de la privacidad, puede traducirse como un avance positivo.

Sin embargo, existe un creciente número de casos donde las cortes deben decidir si el contenido en línea que viola la legislación nacional puede ser eliminado a nivel mundial por las empresas tecnológicas, en lugar de hacerlo solo en ese Estado, lo que genera varias inquietudes, algunas de ellas relativas a la privacidad y la libertad de expresión.

Los Estados deberían considerar con detenimiento la aplicación extraterritorial de la legislación nacional, incluso a través de sentencias judiciales, para asegurar que los PAN y los marcos legales y normativos que adoptan garanticen que las empresas tecnológicas respeten los derechos a la privacidad, la libertad de expresión y la igualdad y no discriminación en los Estados donde operan.

PLANTILLA PARA UNA EVALUACIÓN NACIONAL DE LÍNEA DE BASE (ENLB) DE PAN Y EL SECTOR TECNOLÓGICO

1. MARCO LEGAL Y NORMATIVO

Los Estados deberían evaluar si sus marcos legales y normativos protegen adecuadamente contra las violaciones a los derechos humanos relacionados con el sector tecnológico. Asimismo, los Estados deberían evaluar la medida en que estas leyes y políticas contribuyen a la prevención de dichos abusos.

Si bien las preguntas a continuación se enfocan en los derechos a la privacidad, la libertad de expresión y la igualdad y la no discriminación, también podrían ser desarrolladas con el fin de incluir otros derechos humanos adicionales.

1.1. Normas Internacionales, Regionales y otras

Normas internacionales	¿El Estado ha firmado, ratificado e implementado instrumentos internacionales relevantes de derechos humanos que protejan los derechos a la privacidad, la libertad de expresión y la igualdad y la no discriminación, en particular el Pacto Internacional de Derechos Civiles y Políticos?

	Desde 2011, ¿ha recibido el Estado recomendaciones por parte del Comité de Derechos Humanos de la ONU (o el órgano de tratado que supervisa los instrumentos respectivos) con respecto a la protección de los derechos a la privacidad, la libertad de expresión y la igualdad y la no discriminación relativas a las actividades del sector tecnológico? Si la respuesta es sí, ¿cuál es el progreso en la implementación de las recomendaciones emitidas por este órgano? Desde 2011, ¿ha recibido el Estado recomendaciones por parte de los procedimientos especiales de la ONU o por parte del Examen Periódico Universal relativas a la protección de los derechos a la privacidad, la libertad de expresión o la igualdad y la no discriminación con respecto a las actividades del sector tecnológico? Si la respuesta es sí, ¿cuál es el progreso en la implementación de las recomendaciones emitidas por estos órganos?
Normas regionales	¿El Estado ha firmado, ratificado e implementado instrumentos relevantes de derechos humanos a nivel regional, tales como: • La Convención Americana sobre Derechos Humanos • La Carta Africana de Derechos Humanos y de los Pueblos • La Convención Europea de Derechos Humanos? Desde 2011, ¿ha recibido el Estado recomendaciones por parte de algún organismo regional relativas a la protección de los derechos a la privacidad, la libertad de expresión o la igualdad y la no discriminación con respecto a las actividades del sector tecnológico? Si la respuesta es sí, ¿cuál es el progreso en la implementación de las recomendaciones emitidas por este organismo?

	Desde 2011, ¿ha descubierto alguna corte regional de derechos humanos que el Estado violó su deber de proteger contra los abusos a la privacidad, la libertad de expresión o la igualdad y la no discriminación por parte de alguna empresa tecnológica? Si la respuesta es sí, ¿cuál es el progreso en la implementación de las recomendaciones emitidas por esta corte?
Otras normas	¿El Estado ha firmado, colaborado o respaldado las normas e iniciativas que se mencionan a continuación pertinentes al sector tecnológico y a la privacidad, la libertad de expresión y la igualdad y la no discriminación?: • Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico • Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa • Recomendación N° R(99) 5 del Consejo de Europa sobre la protección de la intimidad en Internet • Recomendación CM/Rec(2020)1 del Comité de Ministros del Consejo de Europa sobre los impactos de los sistemas algorítmicos sobre los derechos humanos • Directrices de la OCDE sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales • Recomendaciones de Ámsterdam sobre la Libertad de Prensa y la Internet de la Organización para la Seguridad y Cooperación en Europa • Declaración de Principios sobre la Libertad de Expresión en África de la Unión Africana • Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones • Principios de Manila sobre responsabilidad legal de los intermediarios • Declaración de Toronto sobre la protección del derecho a la igualdad y la no discriminación en los sistemas de aprendizaje automático • Freedom Online Coalition • Plan de Acción de Rabat

1.2. Leyes y políticas nacionales	
Derecho a la privacidad	¿La Constitución o la legislación garantiza el derecho a la privacidad? ¿Existen excepciones en la legislación que restrinjan el derecho a la privacidad? Si la respuesta es sí: • ¿Son éstas consistentes con limitaciones permisibles dispuestas bajo el derecho internacional y regional de los derechos humanos, es decir, bajo una base legal clara y no discriminatoria, y necesaria y proporcional para alcanzar un objetivo legítimo?
Protección de datos	¿La protección de datos se encuentra regulada? Esto incluye la recopilación, el almacenamiento, el uso y la divulgación de datos personales. Si la respuesta es sí: • ¿es consistente con las mejores prácticas internacionales, como el Reglamento general de protección de datos de la UE? En particular: • ¿cubre todas las formas de datos personales? • ¿cubre a todos los usuarios y personas o solo a los consumidores? • ¿se aplica a todos encargados del tratamiento de datos en los sectores público y privado? • Cuando el consentimiento sea la base legal para el tratamiento de datos, ¿exige que la solicitud de consentimiento sea informada, clara, inteligible, accesible y en un lenguaje sencillo? • ¿permite a las personas solicitar a los encargados del tratamiento de datos copias de sus datos y corregirlos o eliminarlos? • ¿proporciona el derecho a la portabilidad de datos? • ¿incluye el derecho de las personas a no ser objeto de decisiones que tengan efectos significativos que se basen en el tratamiento automatizado? ¿Existe legislación que permita a los gobiernos acceder a los datos almacenados por las empresas

	tecnológicas? (por ejemplo, leyes sobre retención de datos, leyes de metadatos)? ¿Existen mecanismos u organismos nacionales de supervisión que puedan procesar reclamaciones sobre violaciones de datos y que hagan cumplir la legislación sobre protección de datos, tal como una autoridad de protección de datos? Si la respuesta es sí: • ¿cuentan estos organismos con los recursos necesarios? • ¿cuántas violaciones de datos por parte de empresas se han registrado durante los últimos cinco años?
Cifrado	¿Existe alguna ley o política que exija o aliente el uso de cifrado reforzado por parte de las empresas tecnológicas para los datos personales o las comunicaciones? ¿Existe alguna ley o política que restrinja o perjudique la habilidad de las empresas tecnológicas de cifrar datos personales o comunicaciones?
Vigilancia	¿Existe alguna ley o política que regule la vigilancia en línea, intercepción o interferencia de comunicaciones privadas? Si la respuesta es sí: • ¿respeta las mejores prácticas internacionales, como los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones? En particular: • ¿es la ley suficientemente clara y precisa para que las personas tengan un aviso previo y puedan anticipar su aplicación? • ¿se permite la vigilancia solo cuando sea necesaria con el fin de lograr un objetivo legítimo y se lleva a cabo de manera no discriminatoria? • ¿solo autoriza la vigilancia cuando lo permita una autoridad judicial competente, imparcial e independiente?

	• ¿permite a las empresas tecnológicas oponerse o cuestionar exigencias que les hagan las agencias estatales? • ¿limita la transparencia de los informes de las empresas en el contexto de solicitudes de datos por parte del gobierno? • ¿qué evaluación se ha hecho sobre la implementación de la legislación y la participación de las empresas tecnológicas en su implementación?
Libertad de expresión	¿La Constitución o la legislación garantiza el derecho a la libertad de expresión? ¿Existen normas jurídicas sobre la libertad de la información? ¿Existen excepciones en la legislación que restrinjan el derecho a la libertad de expresión? Si es así, ¿respetan las limitaciones permisibles dispuestas bajo el derecho internacional y regional de los derechos humanos, es decir, bajo una base legal clara y no discriminatoria, y necesaria y proporcional para alcanzar un objetivo legítimo? ¿Existe alguna legislación que permita a los gobiernos bloquear o restringir el acceso a Internet?
Regulación de contenidos	¿Existen normas jurídicas o políticas que regulen el contenido en línea o las políticas de moderación de contenidos por parte de las empresas tecnológicas? Si la respuesta es sí: • ¿son coherentes con las mejores prácticas internacionales, como con los Principios de Manila sobre responsabilidad legal de los intermediarios? En particular: • ¿las normas que determinan la responsabilidad de los intermediarios son precisas, claras y accesibles? • ¿eximen a los intermediarios de responsabilidad por el contenido publicado por terceros en circunstancias en las que no han participado en la

	modificación de ese contenido? • ¿garantiza que los intermediarios no sean responsables por no restringir contenido legal? • ¿prohíbe la responsabilidad de los intermediarios por albergar contenido ilegal publicado por terceros? • ¿prohíbe que se exija a los intermediarios que supervisen el contenido de forma proactiva? • ¿asegura que los intermediarios solo estén obligados a restringir el contenido cuando una autoridad judicial independiente e imparcial haya emitido una orden que determine que el material en cuestión es ilegal? • ¿asegura que el intermediario y el proveedor del contenido puedan ejercer un derecho efectivo a ser escuchados (salvo en circunstancias excepcionales)? • ¿impone plazos breves para la supresión de contenido ilícito una vez que se ha informado al intermediario? • ¿impone sanciones económicas elevadas u otras sanciones desproporcionadas por incumplimiento? • ¿existe transparencia sobre las órdenes o solicitudes que las empresas tecnológicas reciben para suprimir contenidos? ¿Existen normas jurídicas o políticas que exijan a las empresas tecnológicas publicar sus políticas de moderación de contenidos en un lenguaje claro y accesible? ¿La Constitución o la legislación garantiza el derecho a la no discriminación?
Igualdad y no discriminación	¿El Estado ha adoptado un marco legal general contra la discriminación? • ¿El marco legal prohíbe la discriminación sobre la base de una normativa no exhaustiva y explícita? • ¿Se prohíben múltiples formas de discriminación, incluyendo la discriminación interseccional? • ¿El marco legal define y prohíbe adecuadamente todas las formas de discriminación reconocidas internacionalmente, a saber, la discriminación directa,

la discriminación indirecta, el acoso y no facilitar el ajuste razonable?
- ¿La protección contra la discriminación es proporcional en todos los ámbitos de la vida regulados por la ley?
- ¿El marco legal impone obligaciones de no discriminación sobre los actores privados?

¿Existe alguna justificación para la discriminación indirecta incluida en el marco legal? De ser así, ¿cumple con las normas internacionales, es decir, tiene un objetivo legítimo y es apropiada y necesaria?

¿Existe alguna justificación para la discriminación directa? Esto solo puede justificarse en circunstancias muy excepcionales, con criterios estrictamente definidos, ya que la discriminación directa rara vez persigue un objetivo legítimo.

¿El marco legal contra la discriminación del Estado exige una acción positiva cuando se identifican desigualdades sustantivas, incluyendo en el acceso y uso de Internet y las nuevas tecnologías?
- ¿El Estado ha implementado políticas de acción positiva para acceder y utilizar Internet y las nuevas tecnologías?

¿El Estado incorpora evaluaciones de impacto en la igualdad como un elemento integral de sus políticas? ¿Están las evaluaciones del impacto en la igualdad destinadas a identificar y eliminar los efectos discriminatorios reales o potenciales de las políticas estatales?
¿Se exige o se espera de las empresas, incluidas las empresas tecnológicas, que lleven a cabo la debida diligencia en materia de derechos humanos u otros procesos de debida diligencia, tales como protección de datos y evaluaciones de impacto en la igualdad, incluyendo evaluar e informar en sus impactos negativos sobre los derechos humanos? Si la respuesta es sí:
- ¿proporciona el Estado alguna orientación o metodología requerida para los procesos de debida diligencia?

Debida diligencia	¿Se exige o se espera de las empresas, incluidas las empresas tecnológicas, que lleven a cabo la debida diligencia en materia de derechos humanos u otros procesos de debida diligencia, tales como protección de datos y evaluaciones de impacto en la igualdad, incluyendo evaluar e informar en sus impactos negativos sobre los derechos humanos? Si la respuesta es sí: • ¿proporciona el Estado alguna orientación o metodología requerida para los procesos de debida diligencia?

2. LA RESPONSABILIDAD DEL SECTOR TECNOLÓGICO DE RESPETAR LOS DERECHOS HUMANOS

Según el Pilar II de los PRNU, las empresas tecnológicas tienen la responsabilidad de respetar los derechos humanos y de proceder con adecuada debida diligencia en materia de derechos humanos. Los Estados deberían evaluar hasta qué punto las empresas tecnológicas cumplen con esta responsabilidad y si aplican los derechos humanos en sus políticas y operaciones.

Las preguntas a continuación pueden ser utilizadas para recopilar información desde las empresas tecnológicas sobre sus políticas y procedimientos de gestión para respetar los derechos humanos en concordancia con las expectativas fijadas en el Pilar II de los PRNU. Éstas pueden ser adaptadas al tipo de empresa de que se trate (empresa multinacional, pyme, empresa estatal, empresa que cotiza en la bolsa) y también se pueden expandir para incluir cuestiones relativas a los derechos humanos más allá de la privacidad, la libertad de expresión, y la igualdad y la no discriminación.

2.1. Gobernanza

Compromiso público	¿Tienen las empresas tecnológicas en el Estado un compromiso público de respetar los derechos humanos? Si la respuesta es sí: • ¿el compromiso está incluido en (i) una política autónoma de derechos humanos, (ii) en otra política como una de sostenibilidad o responsabilidad social corporativa?

	¿Las empresas tecnológicas en el Estado se han suscrito a iniciativas de múltiples partes interesadas con un componente de derechos humanos como la Global Network Initiative o el Pacto Mundial de la ONU?
Supervisión de la gobernanza y la gestión	¿Los altos directivos de las empresas tecnológicas supervisan la forma en que sus políticas y prácticas afectan los derechos humanos? ¿El compromiso público de respetar los derechos humanos se integra en todas las funciones y operaciones comerciales?
Implementación interna	¿Las empresas tecnológicas cuentan con mecanismos para implementar sus compromisos con los derechos humanos?
2.2. Derechos humanos específicos	
Derecho a la privacidad	¿Las políticas y los compromisos de las empresas tecnológicas demuestran formas concretas en las que respetan el derecho a la privacidad de los usuarios?
Protección de datos	¿Las empresas tecnológicas proporcionan políticas de protección de datos claras y accesibles para los usuarios? ¿Las empresas tecnológicas notifican a los usuarios cuando modifican sus políticas de privacidad? Las políticas de protección de datos: • ¿revelan claramente qué datos personales se recopilan y tratan, y la forma en que se hace? • ¿buscan el consentimiento informado de los usuarios para la recopilación, el tratamiento y el intercambio de datos?

	• ¿revelan claramente qué datos personales se comparten y con quién? • ¿comunican claramente las finalidades para los que se recopilan, tratan y comparten los datos personales? • ¿revelan claramente por cuánto tiempo se conservan los datos personales? • ¿presentan claramente a los usuarios cómo pueden ejercer control sobre la recopilación, tratamiento e intercambio de sus datos personales? • ¿permiten a los usuarios obtener copias de sus datos personales? • ¿permiten a los usuarios que sus datos personales de sean corregidos o eliminados?
Protección de datos	Las empresas tecnológicas: • ¿comunican de forma clara la información sobre sus procesos institucionales para garantizar la seguridad de sus productos y servicios? • ¿abordan las vulnerabilidades de seguridad cuando se descubren? • ¿comunican públicamente información sobre sus procesos de respuesta a violaciones de datos? • ¿cifran la comunicación del usuario y el contenido privado para que los usuarios puedan controlar quién tiene acceso?
Libertad de expresión	¿Las políticas y compromisos de las empresas tecnológicas incluyen formas concretas de respetar el derecho de los usuarios a la libertad de expresión?
Moderación de contenidos	Las empresas tecnológicas: • ¿publican políticas de moderación de contenidos claras y accesibles? • ¿proporcionan notificaciones a los usuarios cuando cambian sus políticas de moderación de contenidos?

	• ¿divulgan y publican regularmente datos sobre el volumen y la naturaleza de las acciones tomadas para estringir el contenido o las cuentas que violan las políticas de moderación de contenidos? • ¿notifican a los usuarios cuando restringen contenido o cuentas? Las empresas tecnológicas: • ¿informan sobre su proceso para responder a solicitudes gubernamentales (incluidas órdenes judiciales) y solicitudes privadas para suprimir contenido o cuentas? • ¿publican regularmente datos sobre solicitudes gubernamentales (incluidas órdenes judiciales) y solicitudes privadas para suprimir contenido o cuentas?
No discriminación	¿Las empresas tecnológicas adoptan políticas de no discriminación que abarquen todas las áreas de actividad, incluida la disposición de servicios en línea y otros servicios digitales? ¿Las empresas tecnológicas proporcionan una adecuada formación y sensibilización sobre el derecho a la no discriminación a todo su personal y demás agentes? ¿Las empresas tecnológicas integran evaluaciones de impacto en la igualdad durante el diseño y despliegue de sus productos y servicios? • ¿Las empresas tecnológicas aseguran que las evaluaciones de impacto en la igualdad son un elemento esencial de la evaluación de sus productos? ¿Adoptan las empresas tecnológicas políticas para garantizar que se proporcionen ajustes razonables cuando sea necesario? ¿Las empresas tecnológicas garantizan y promueven la igualdad de accesibilidad a sus servicios?

3. REPARACIÓN Y REMEDIO

Los Estados deben evaluar qué mecanismos judiciales y extrajudiciales están a disposición de las personas afectadas por empresas tecnológicas, así como la efectividad de éstos.

3.1. Mecanismos estatales

Mecanismos judiciales	¿Existen recursos judiciales asequibles, rápidos y efectivos ante tribunales independientes e imparciales aplicables ante violaciones de derechos humanos relacionadas con el sector tecnológico?
Accesibilidad a la reparación	¿Es accesible la justicia para las víctimas de violaciones de derechos humanos relacionadas con el sector tecnológico, teniendo en cuenta diversas situaciones y necesidades, incluyendo, por ejemplo, barreras geográficas, lingüísticas y culturales? ¿Las normas legales relacionadas con la evidencia y las pruebas garantizan que las víctimas de violaciones sobre sus derechos humanos relacionadas con el sector tecnológico no se vean indebidamente inhibidas para obtener reparación? • En los procesos civiles, ¿se adaptan las normas probatorias para asegurar que cuando las personas aleguen haber sido objeto de hechos por los que se pueda presumir que ha existido discriminación (caso prima facie), corresponda al demandado probar que no se ha vulnerado el derecho a la no discriminación? ¿Son proporcionales las formas de apoyo financiero o de otro tipo para las personas o grupos que hayan sido víctimas de violaciones de derechos humanos relacionadas con el sector tecnológico, por ejemplo, a través de asistencia jurídica? Si es así, ¿quién es elegible para estas formas de apoyo financiero o de otro tipo? ¿Existe asesoramiento y asistencia legal disponible

	para personas o grupos que hayan sido víctimas de violaciones de derechos humanos relacionadas con el sector tecnológico? Si es así, ¿quién es elegible para estas formas de asistencia jurídica y legal? ¿Son posibles las reclamaciones colectivas, demandas colectivas y otras formas de litigio colectivo donde ha habido violaciones de derechos humanos por parte del sector tecnológico que afecten a varias personas? ¿Existen medidas adecuadas para asegurar que las personas estén protegidas de cualquier tratamiento o consecuencia adversa en respuesta a la presentación de una denuncia por violaciones de derechos humanos por parte del sector tecnológico?
Acceso a la información	¿El Estado facilita el acceso a la información en relación con los mecanismos de reparación disponibles? Si la respuesta es sí: • ¿es esta información fácilmente accesible y asimilable?
Mecanismos estatales no judiciales	¿Existen políticas para promover el acceso a mecanismos de reclamación estatal no judicial, tales como una autoridad de protección de datos, una institución nacional de derechos humanos o una Defensoría del Pueblo? Si la respuesta es sí: • ¿son estos mecanismos legítimos, independientes, accesibles, predecibles, equitativos, transparentes y compatibles con los derechos? ¿Existen reclamaciones ante un PNC de la OCDE? Si hubieran, ¿las hay sobre empresas tecnológicas? ¿Han existido reclamaciones o inquietudes llevadas ante la institución nacional de derechos humanos? Si existe alguna, ¿se relaciona con empresas tecnológicas?

Reparaciones y sanciones	¿Pueden los mecanismos judiciales y no judiciales proporcionar reparaciones efectivas, incluyendo sanciones, por violaciones de derechos humanos relacionadas con el sector tecnológico? • ¿Se aplican eficazmente dichos recursos y/o sanciones?
3.2. Mecanismos no estatales	
Empresas tecnológicas	¿Las empresas tecnológicas proporcionan mecanismos de reclamación y reparación accesibles para abordar las inquietudes de derechos humanos de los usuarios? ¿Son estos mecanismos legítimos, independientes, accesibles, predecibles, equitativos, transparentes y compatibles con los derechos, en concordancia con los criterios de efectividad de los PRNU?
3.3. Extraterritorialidad	
Extraterritorialidad	¿El Estado ejerce jurisdicción extraterritorial sobre las acciones de empresas con sede o registradas en ellos, o sus subsidiarias, por violaciones de los derechos humanos cometidas en el exterior, particularmente en relación con las operaciones del sector tecnológico? Por el contrario, ¿el Estado ejerce control sobre las empresas tecnológicas registradas en el extranjero que operan en su jurisdicción? ¿Se someten las empresas tecnológicas globales o extranjeras a las jurisdicciones de los tribunales nacionales?

Lista de verificación de PAN y el sector tecnológico

La Lista de verificación a continuación contiene los elementos mínimos necesarios para que los Estados aseguren que las implicancias del sector tecnológico sobre los derechos humanos sean tomadas en consideración de forma adecuada al momento de comenzar el proceso de desarrollo, evaluación o revisión de un PAN. Ha sido diseñada de acuerdo con la Lista de verificación de PANs que se encuentra en el Kit de herramientas de DIHR-ICAR.

1. Gobernanza y recursos

• Identificar todos los departamentos gubernamentales, agencias y otros organismos públicos e instituciones que tengan un mandato pertinente a la tecnología, el sector tecnológico y/o la privacidad, la libertad de expresión, y la igualdad y la no discriminación, y asegurar que se encuentren incluidos en todas las etapas del proceso del PAN. Estas deben incluir, cuando existan, no solo los departamentos gubernamentales pertinentes, sino también organismos reguladores, instituciones nacionales de derechos humanos, Defensorías del Pueblo y agencias de protección de datos.

• Asignar los recursos necesarios a dichos departamentos, agencias, organismos e instituciones, para así garantizar que desempeñen un papel activo en el mapeo de las partes interesadas, en las consultas, en la disposición de desarrollo de capacidades y en la formulación de políticas.

2. Mapeo y participación de las partes interesadas

• Como parte del mapeo general de las partes interesadas, elaborar un mapeo de todos los actores no estatales que tengan conocimiento y/o estén interesados en el desarrollo de políticas relativas a la tecnología, el sector tecnológico y/o la privacidad, la libertad de expresión, y la igualdad y la no discriminación.

• Facilitar la participación significativa de estos actores, asegurando la representación de intereses múltiples y diversos, asignando los recursos adecuados y desarrollando capacidades cuando sea necesario.

• Identificar a aquellos que estén en mayor riesgo de sufrir impactos negativos y discriminatorios en cuanto a la privacidad y la libertad de expresión, y asegurar que puedan participar en el proceso considerando sus necesidades específicas y sus debilidades.

3. Evaluación de línea de base nacional

• Garantizar que la organización que elabore la ENLB tenga los conocimientos sobre el sector tecnológico y sobre cuestiones relativas a la privacidad, la libertad de expresión, y la igualdad y la no discriminación.

• Incluir preguntas específicas sobre el sector tecnológico y la privacidad, la libertad de expresión, y la igualdad y la no discriminación dentro de la ENLB, incorporando los resultados de la ENLB de PAN y el sector tecnológico en este suplemento temático.

• Identificar lagunas de políticas y de regulación, y los riesgos más importantes en la privacidad, la libertad de expresión y la igualdad y la no discriminación.

4. Alcance, contenido y prioridades

• Al considerar el alcance de la jurisdicción estatal, tomar en consideración la importancia de la extraterritorialidad con respecto a las operaciones del sector tecnológico.

• Priorizar las acciones relativas a los impactos más graves del sector tecnológico y garantizar que todos los compromisos en relación con la industria sean específicos, medibles, alcanzables, relevantes y acotados en el tiempo.

5. Rendición de cuentas y seguimiento

• Publicar información acerca de la ENLB y del PAN en un formato accesible y sencillo de entender, en idiomas compartidos por todas las partes interesadas, asegurando que cualquier parte interesada afectada por el sector tecnológico que haya sido consultada entienda de qué manera su aporte fue considerado.

• Incluir las partes interesadas que hayan sido incorporadas en el marco para el seguimiento y la presentación de informes sobre la implementación de acciones relativas al sector tecnológico en del PAN, incluyendo cualquier otra formulación de políticas.

ANEXO 1: El sector tecnológico en PAN Actuales

ESTADO	COMPROMISO(S)
República Checa (2017) 	No es posible encontrar compromisos relativos al sector tecnológico dentro del PAN de la República Checa. En su lugar, se refiere a la tecnología solo en el contexto del acceso a la justicia y las cortes, destacando que el sistema judicial puede beneficiarse de las ventajas que ofrece la tecnología avanzada.
Finlandia (2014) 	El PAN finlandés destaca que "la protección de la privacidad que se encuentra particularmente relacionada con comunicaciones electrónicas ha recibido bastante atención en las discusiones públicas recientes" y que "las preguntas de privacidad relativas a las comunicaciones electrónicas son especialmente importantes en Finlandia, donde la infraestructura de las tecnologías de la información y comunicación posee una sólida posición". [cita traducida] El PAN se compromete a organizar "una mesa redonda (...) sobre cómo asegurar la protección de la privacidad en Finlandia con las autoridades, las empresas de TIC y la sociedad civil". [cita traducida]
Irlanda (2017) 	No es posible encontrar compromisos específicos sobre el sector tecnológico dentro del PAN irlandés. Sin embargo, sí se refiere al hecho de que hay un gran número de empresas tecnológicas multinacionales en Irlanda, y que el Comisionado sobre la protección de datos del país tiene la responsabilidad de supervisar grandes cantidades de datos y ha estado involucrado en casos de alta connotación. El PAN señala que el gobierno se compromete a respaldar al Comisionado de datos y que han cuadruplicado los fondos para su trabajo.
Luxemburgo (2018) 	No es posible encontrar compromisos específicos sobre el sector tecnológico dentro del PAN de Luxemburgo. En cambio, el PAN simplemente señala que "el riesgo potencial de impactos negativos sobre los derechos humanos que las actividades del sector privado puedan tener... – incluyendo las tecnologías de la información y la comunicación – incluyendo en el área de la inteligencia artificial – protección de datos ..." [cita traducida].

Polonia (2017) 	El PAN polaco se compromete a crear un “proyecto de Reglamento para luchar contra las restricciones a la libertad de expresión, por una parte, y para bloquear el contenido ilegal en Internet, por la otra” [cita traducida]. Estas regulaciones podrían clarificar el procedimiento de notificación y eliminación de contenido ilegal en línea y, a su vez, fortalecer salvaguardias legales para la libertad de expresión en las actividades de proveedores de servicios electrónicos.
Suecia (2015) 	No es posible encontrar compromisos específicos sobre el sector tecnológico dentro del PAN sueco. Sin embargo, sí señala que: “La libertad y privacidad en Internet se encuentran dentro de las grandes problemáticas mundiales del futuro. Es fundamental para Suecia que los derechos humanos que aplican fuera de línea también lo hagan en línea”. [cita traducida] El PAN señala que Suecia contribuyó a garantizar que las Líneas directrices de la OCDE para empresas multinacionales ahora exhorten a las empresas a que apoyen a los derechos humanos en Internet, y que Suecia se encontraba dentro del grupo de países que presentaron resoluciones sobre la libertad en Internet en el Consejo de Derechos Humanos de la ONU en 2012 y en 2014.
Suiza (2016) 	No es posible encontrar compromisos específicos sobre el sector tecnológico dentro del PAN suizo. Sin embargo, se refiere al potencial para que las “tecnologías para la vigilancia de Internet y comunicación móvil” sean utilizadas tanto con propósitos civiles como militares. Añade que “la exportación o el corretaje de tecnologías para la vigilancia de internet y las comunicaciones móviles se rige bajo la normativa sobre el control de mercancías” y que “la transferencia de propiedad intelectual, incluyendo conocimientos y la concesión de derechos, en relación con las tecnologías para la vigilancia de Internet y comunicaciones móviles, también se somete a licencia”. [cita traducida]
Tailandia (2019) 	El PAN tailandés se enfoca, principalmente, en la tecnología en el contexto laboral. Señala que un desafío clave en esta área es “proteger la mano de obra de su sustitución por la tecnología”. [cita traducida] Dentro de la lista de actividades planeadas, el PAN incluye

	“elaborar planes o medidas para apoyar reparaciones y ayudar a los grupos de trabajadores despedidos de acuerdo con las normas de reparación establecidas”. El Ministerio de Trabajo es el encargado de esta actividad, con un plazo desde el año 2019 al 2022.
Reino Unido (2013 y 2016) 	El PAN del Reino Unido se compromete a “desarrollar directrices con el fin de abordar los riesgos que crean las exportaciones de información y la tecnología de las comunicaciones que no son sujetas a control de exportación, pero que podrían tener impactos en los derechos humanos, incluyendo la libertad de expresión en línea”. [cita traducida] En 2014, el Gobierno del Reino Unido junto a techUK (asociación de comercio de tecnología), y el Institute for Human Rights and Business, publicaron “Assessing Cyber Security Export Risks: Human Rights and National Security”.
Estados Unidos (2016) 	El PAN estadounidense señala que: “El impacto y la importancia de la conducta empresarial en el sector de las tecnologías de la información y la comunicación ha crecido, dado que, cada vez más frecuentemente, las interacciones sociales, comerciales, educacionales y recreacionales tienen lugar en línea”. [cita traducida] El PAN compromete al gobierno de los Estados Unidos a “trabajar con otras agencias y partes interesadas, con el fin de desarrollar un mecanismo permanente para identificar, documentar y publicar lecciones aprendidas y las mejores prácticas relativas a las acciones empresariales que promuevan y protejan los derechos humanos en línea”. También compromete al gobierno a “fomentar la participación constante de las partes interesadas relevantes para apoyar el diálogo y la colaboración en relación con el respeto de los derechos humanos en el sector las TIC”. [cita traducida]

NOTAS FINALES

1 Véase, por ejemplo, Consejo de Derechos Humanos de la ONU, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Doc. A/HRC/35/22, 30 de marzo de 2017; Consejo de Derechos Humanos de la ONU, Informe del Relator Especial sobre el derecho a la privacidad, Doc. A/HRC/40/63, 27 febrero de 2019; Consejo de Derechos Humanos de la ONU, Informe del Relator Especial sobre la extrema pobreza y los derechos humanos, A/74/493, 11 octubre de 2019 y Jørgensen, R. F., Human Rights in the Age of Platforms ed., MIT Press, 2019.

2 Mesa Redonda Internacional para la Rendición de Cuentas Empresarial y el Instituto Danés de Derechos Humanos, Kit de herramientas sobre planes de acción nacionales de empresas y derechos humanos, edición 2017, 2017, disponible en: https://www.humanrights.dk/sites/humanrights.dk/files/media/migrated/dihr_icar_nap_toolkit_may_15_2018_spanish.pdf

3 Para cifras actualizadas, revisar Global Naps, disponible en: https://globalnaps.org/.

4 Véase más adelante, en la Sección 1.3.

5 Una base de datos sobre dichas acciones legales se puede encontrar en el Digital Watch Observatory of the Geneva Internet Platform, disponible en: https://dig.watch/trends/uber.

6 Consejo de Derechos Humanos de la ONU, Resolución 34/7. El derecho a la privacidad en la era digital, Doc. ONU A/HRC/RES/34/7, 7 de abril de 2017.

7 Comité de Derechos Humanos de la ONU, Observación general N°18: No discriminación, DOC. ONU HRI/GEN/1/Rev.9 (Vol. I), 10 de noviembre de 1989.

8 Para las cifras más actualizadas, véase Global Naps, disponible en: https://globalnaps.org/.

9 En mayo de 2016, el Reino Unido actualizó su primer PAN (adoptado en 2013), y presentó las medidas que se tomaron para cumplir los compromisos adquiridos en el primer PAN, incluidas aquellas relativas al sector tecnológico: HM Government, Good Business: Implementing the UN Guiding Principles on Business and Human Rights, actualizado en mayo de 2016, disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/522805/Good_Business_Implementing_the_UN_Guiding_Principles_on_Business_and_Human_Rights_updated_May_2016.pdf.

10 La falta de compromisos y acciones SMART en los PAN ha sido señalada en general. Véase, por ejemplo, Instituto Danés de Derechos Humanos, National Action Plans & Business and Human Rights: An Analysis of Plans from 2013 - 2018, 2018, págs. 21-23, disponible en: https://mk0globalnapshvllfq4.kinstacdn.com/wp-content/uploads/2018/11/nap-analysis-full-report.pdf.

11 Véase, por ejemplo, Kreps, S. E., Social Networks and Technology in the

Prevention of Crimes against Humanity" in Rotberg, R.R. (ed.), Mass Atrocity Crimes: Preventing Future Outrages, World Peace Foundation, 2010; Hargreav4rtg56|es, C. y Hattotuwa, S., ICTs for the Prevention of Mass Atrocity Crimes, ICT for Peace Foundation, octubre de 2010, disponible en: http://ict4peace.org/wp-content/uploads/2010/11/ICTs-for-the-Prevention-of-Mass-Atrocity-Crimes1.pdf.

12 Véase, por ejemplo, Amnistía Internacional, Gigantes de la Vigilancia, 2019, disponible en: https://www.amnesty.org/es/latest/news/2019/11/google-facebook-surveillance-privacy/

13 Consejo de Derechos Humanos de la ONU, Informe del Relator Especial sobre el derecho a la privacidad, Doc. ONU A/72/43103, 19 de octubre de 2017, párr. 75. [Disponible en inglés]

14 Ibid.

15 Véase, por ejemplo, Amnistía Internacional, Gigantes de la Vigilancia, 2019, disponible en: https://www.amnesty.org/es/latest/news/2019/11/google-facebook-surveillance-privacy/

16 Véase, por ejemplo, la investigación llevada a cabo por el Centro de derechos humanos de la Universidad de Essex, Big Data and Technology project, disponible en: https://www.hrbdt.ac.uk/.

17 Véase Borgesius, F. Z., Discrimination, Artificial Intelligence, and Algorithmic Decision-Making, Directorate General of Democracy, Consejo de Europa, 2018, disponible en: https://rm.coe.int/discrimination- artificial-intelligence-and-algorithmic-decision-making/1680925d73.

18 Ibid.

19 Dastin, J., "Amazon scraps secret AI recruiting tool that showed bias against women", Reuters, 10 de octubre de 2018, disponible en: https://www.reuters.com/article/us-amazon-com-jobs-automation-in...-ai-recruiting- tool-thatshowed-bias-against-women-idUSKCN1MK08G.

20 Ibid.

21 Comisión Federal de Comercio, Data Brokers: A Call for Transparency and Accountability, mayo de 2014, disponible en: https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

22 Angwin, J., Tobin, A. and Varner, M., "Facebook (Still) Letting Housing Advertisers Exclude Users by Race", ProPublica, noviembre 2017, disponible en: https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin. En marzo de 2019, Facebook anunció que aplicaría restricciones a las opciones de segmentación de anuncios de viviendas, empleos y crédito en Estados Unidos después de llegar a un acuerdo con organizaciones de derechos civiles.

23 Angwin, J. et al., "Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks", ProPublica, 23 de mayo de 2016, disponible en: https://www.ProPublica.org/article/machine-bias-

riskassessments-in-criminal-sentencing.
24 Confessore, N., “Cambridge Analytica and Facebook: the scandal so far”, The New York Times, 4 de abril de 2018, disponible en: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
25 Perlroth, N., “All 3 Billion Yahoo Accounts Were Affected by 2013 Attack”, The New York Times, 3 de octubre de 2017, disponible en: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.
26 Human Rights Watch, Lado oscuro: Orígenes secretos de las pruebas en causas penales en EE. UU., disponible [en inglés] en: https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.
27 Véase una lista de casos en el Centro de Información sobre Empresas y Derechos Humanos, Corporate Legal Accountability Hub, disponible en https://www.business-humanrights.org/en/corporate-legal-accountability/case-profiles/industry/technology.
28 Human Rights Watch, China: Big Data Fuels Crackdown in Minority Region, disponible en: https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region.
29 Freedom House, Freedom on the Net 2018, The Rise of Digital Authoritarianism, disponible en: https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.
30 Ibid.
31 Véase https://necessaryandproportionate.org/principles.
32 Véase https://www.reformgovernmentsurveillance.com.
33 Five Country Ministerial, Statement of Principles on Access to Evidence and Encryption, disponible en: https://www.ag.gov.au/About/CommitteesandCouncils/Documents/joint-statement-principles-access-evidence.pdf.
34 El Consejo Europeo de Protección de Datos, Opinión 5/2019 sobre la relación existente entre la Directiva sobre la privacidad y las comunicaciones electrónicas y el RGPD, en particular en relación con la competencia, funciones y poderes de las autoridades de protección de datos, 12 de marzo de 2019, disponible [en inglés] en: https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf.
35 La Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo del 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, que deroga la Decisión Marco 2008/977/JAI del Consejo, disponible en: https://eur-lex.europa.eu/eli/dir/2016/680/oj.
36 Comité Europeo de Protección de Datos, 1 year GDPR - taking stock, 22 de

mayo de 2019, disponible en: https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en.

37 Commission Nationale de l'Informatique et des Libertés, The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 de enero de 2019, disponible en: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

38 Véase la propuesta de Equal Rights Trust al Relator Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia en relación con las amenazas graves y estructurales que las nuevas tecnologías de la información, como el big data, el aprendizaje automático y la inteligencia artificial, plantean a los derechos a la no discriminación y a la igualdad racial, principios y estándares de derechos humanos, disponible [en inglés] en: https://www.equalrightstrust.org/news/equal-rights-trusts-submission-un-special-rapporteur-contemporary-forms-racism.

39 Access Now, The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems, disponible en: https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-no-discrimination-in-machine-learning-systems/.

40 Consejo de Derechos Humanos de la ONU, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Doc. A/73/348, 29 de agosto de 2018, párr. 12.

41 Véase, por ejemplo, el estudio del año 2019 encargado por el Departamento de Políticas para los Derechos de los Ciudadanos y Asuntos Constitucionales, Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, febrero 2019, disponible en: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf.

42 Amnistía Internacional, Toxic Twitter: A Toxic Place for Women, marzo 2018, disponible en: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.

43 Consejo de Derechos Humanos de la ONU, Report of the independent international fact-finding mission on Myanmar, UN Doc. A/HRC/39/64, 12 de septiembre de 2019, párr. 74. El informe hace referencia explícita al rol de Facebook en la difusión del discurso de odio entre los rohingya en Myanmar.

44 Ibid.

45 Access Now, The State of Internet Shutdowns Around the World: #KeepItOn Report, disponible en: https://www.accessnow.org/keepiton/.

46 Ibid.

47 Global Network Initiative, Disconnected: A Human Rights-Based Approach to Network Disruptions, junio de 2018, disponible en: https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf.

48 Weidmann, N. B., Benitez-Baleato, S., Hunziker, P., Glatz, E. and Dimitropoulos, X. (2016), Digital discrimination: Political bias in Internet service provision across ethnic groups. Science, 353(6304), 1151-1155.

49 Consejo de Derechos Humanos de la ONU, Resolución 32/13. Promoción,

protección y disfrute de los derechos humanos en Internet, Doc. ONU A/HRC/RES/32/13, 18 de julio de 2016.

50 Véase, por ejemplo, Consejo de Derechos Humanos de la ONU, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Doc. ONU A/HRC/35/22, 30 de marzo de 2017.

51 Electronic Frontier Foundation, NGO Community Urges ICANN to Scrutinize the.ORG Sale, marzo 2020, 9 de marzo de 2020, disponible en: https://www.eff.org/deeplinks/2020/03/ngo-community-urges-icann-scrutinize-org-sale.

52 Población digital a nivel mundial hasta enero de 2020, https://www.statista.com/statistics/617136/digital-population-worldwide/.

53 Consejo de Derechos Humanos de la ONU, Resolución 32/13. Promoción, protección y disfrute de los derechos humanos en Internet, Doc. ONU A/HRC/RES/32/13, 18 de julio de 2016.

54 BBC, Websites to be fined over 'online harms' under new proposals, 8 de abril de 2019, disponible en: https://www.bbc.com/news/technology-47826946.

55 Freedom on the Net 2018, The Rise of Digital Authoritarianism, pág. 2, disponible en: https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20Booklet_11_1_2018.pdf.

56 Véase, por ejemplo, Electronic Frontier Foundation, EFF, Human Rights Watch, and Over 70 Civil Society Groups Ask Mark Zuckerberg to Provide All Users with Mechanism to Appeal Content Censorship on Facebook, 13 de noviembre de 2018, disponible en: https://www.eff.org/press/releases/eff-human-rights-watch-and-over-70-civil-society-groups-ask-mark-zuckerberg-provide.

57 Consejo de Derechos Humanos de la ONU, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Doc. ONU A/HRC/38/35, 6 de abril de 2018, párr. 27.

58 Véase, por ejemplo, Article 19, Facebook Community Standards: Analysis against international standards on freedom of expression, 30 de julio de 2018, disponible en: https://www.article19.org/resources/facebook-community-standards-analysis-against-international-standards-on-freedom-of-expression/; Article 19, Twitter Rules: Analysis against international standards on freedom of expression, 6 de septiembre de 2018, disponible en https://www.article19.org/resources/twitter-rules-analysis-against-international-standards-on-freedom-of-expression.

59 Consejo de Derechos Humanos de la ONU, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Doc. A/73/348, 29 de agosto de 2018, párr. 15.

60 Véase https://santaclaraprinciples.org.

61 Véase https://www.manilaprinciples.org.

62 Consejo de Derechos Humanos de la ONU, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Doc. ONU A/HRC/38/35, 6 de abril de 2018, párrs. 41-63.

63 Ibid., párr. 48.

64 Article 19, The Social Media Councils Consultation Paper, junio 2019,

disponible en https://www.article19.org/wp-content/uploads/2019/06/A19-SMC-Consultation-paper-2019-v05.pdf

65 Facebook, Preparing the Way Forward for Facebook's Oversight Board, 28 de enero de 2020, disponible en https://about.fb.com/news/2020/01/facebooks-oversight-board/.

66 Horowitz, J., In Italian Schools, Reading, Writing and Recognizing Fake News, The New York Times, 18 de octubre de 2017, disponible en: https://www.nytimes.com/2017/10/18/world/europe/italy-fake-news.html.

67 Apple, Apple teams with media literacy programs in the US and Europe, 19 de marzo de 2019, disponible en: https://www.apple.com/uk/newsroom/2019/03/apple-teams-with-media-literacy-programs-in-the-us-and-europe/.

68 Freedom House, Freedom on the Net 2018, The Rise of Digital Authoritarianism, disponible en: https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.

69 Ibid.

70 Mesa Redonda Internacional para la Rendición de Cuentas Empresarial y el Instituto Danés de Derechos Humanos, Kit de herramientas sobre planes de acción nacionales de empresas y derechos humanos, edición 2017, 2017, disponible en: https://www.humanrights.dk/sites/humanrights.dk/files/media/migrated/dihr_icar_nap_toolkit_may_15_2018_spanish.pdf, Sección 2.1.7

71 Mesa Redonda Internacional para la Rendición de Cuentas Empresarial y el Instituto Danés de Derechos Humanos, Kit de herramientas sobre planes de acción nacionales de empresas y derechos humanos, edición 2017, 2017, disponible en: https://www.humanrights.dk/sites/humanrights.dk/files/media/migrated/dihr_icar_nap_toolkit_may_15_2018_spanish.pdf, Sección 2.2. 72 Una evaluación de impacto sectorial (SWIA, por sus siglas en inglés) tiene como objetivo evaluar los impactos potenciales de un sector empresarial en específico en un contexto geográfico en particular. De este modo, una SWIA (a) aborda múltiples niveles de análisis; (b) apunta a modelar políticas, leyes y proyectos; (c) involucra investigación de campo exhaustiva; (d) adopta un amplio enfoque sobre los impactos en los derechos humanos, y (e) sirve como un recurso público. Véase, por ejemplo, la Evaluación de impacto sectorial de Myanmar sobre el sector de las tecnologías de la información realizada por El Centro de Myanmar para Negocios Responsables, disponible [en inglés] en: https://www.myanmar-responsiblebusiness.org/sectors/ict.html.