Vigilancia biométrica remota en América Latina:

¿las empresas están respetando los derechos humanos?

¿Qué les preguntamos a las empresas?

En agosto de 2021, Access Now, Asociación por los Derechos Civiles (ADC, Argentina), Laboratorio de Políticas Públicas e Internet (LAPIN, Brasil) y LaLibre.net (Ecuador), lanzaron el informe "Tecnología de vigilancia en América Latina: hecha en el exterior, utilizada en casa", que se centra en la venta y el uso de las tecnologías de vigilancia biométrica remota en la región. Antes de dicha publicación, les dimos a todas las empresas involucradas la oportunidad de compartir su perspectiva, pero ninguna de ellas eligió hacerlo.

En 2022, Access Now amplió su trabajo sobre este tema con el lanzamiento de la campaña #PorQuéNosVigilan, que aborda los peligros que conlleva la implementación de tecnologías de vigilancia masiva en los distintos países de América Latina. A su vez, Access Now se asoció con el Centro de Información sobre Empresas y Derechos Humanos para obtener respuestas de las empresas que implementan tecnologías de vigilancia en la región. Como resultado, solo nueve de las 23

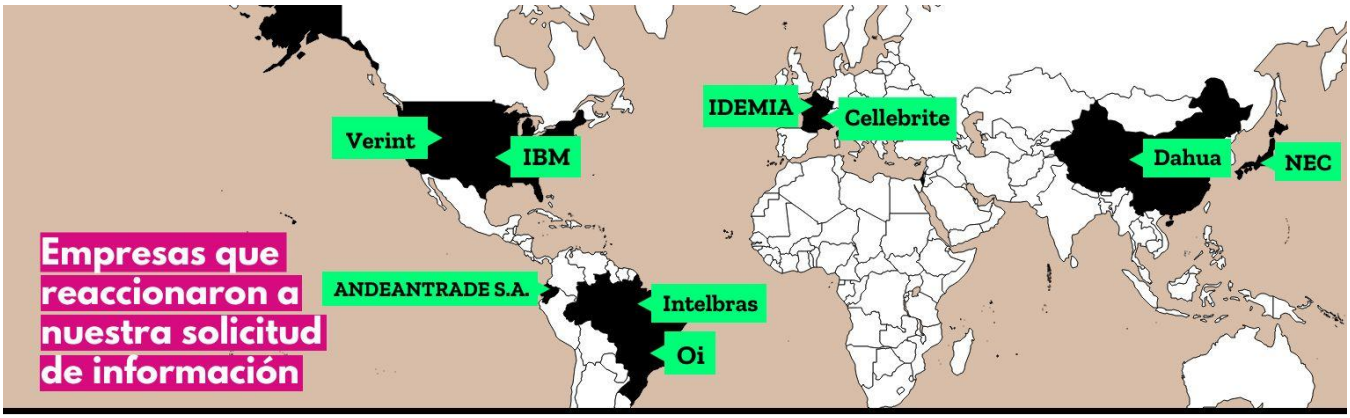
empresas que mencionamos en nuestro informe de 2021 reaccionaron, mientras que las 14 restantes permanecieron en silencio.

La cantidad limitada de respuestas que recibimos no terminó de esclarecer el alcance de las tecnologías con capacidades de vigilancia implementadas en la región. La mayoría de las empresas solo brindaron respuestas generales, en lugar de responder cada una de nuestras preguntas específicas. También notamos que algunas respuestas sugieren que las empresas no cumplen con los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas (PRNU), en especial, en cuanto al compromiso de respetar los derechos humanos, los procesos de debida diligencia implementados para identificar y prevenir los perjuicios significativos a los derechos humanos y la divulgación abierta de información sobre el cumplimiento actual de las leyes vigentes.

Las empresas deben comunicar al público de manera abierta y transparente las medidas que toman para amortiguar el impacto que sus actividades pueden tener en los derechos humanos, en particular, cuando surgen inquietudes, ya sea de manera directa o indirecta, por parte de las comunidades y los individuos afectados. El silencio a la hora de responder sobre estos temas es una manera de evadir la responsabilidad, así como impedir que especialistas independientes en el tema evalúen sus actividades.

En el siguiente artículo, analizamos las respuestas que recibimos y en qué medida la información proporcionada se alinea con los PRNU.

Empresas que respondieron nuestro pedido de información



- **ANDEANTRADE S.A**
- BGH Tech Partner
- **Cellebrite**
- **Dahua**
- Danaide
- El Corte Inglés
- Full Tecnología FullTec CIA. LTDA
- Hikvision
- Huawei
- IAFIS Argentina S.A
- **IBM**
- **Idemia (former Morpho)**
- **Intelbras**
- Johnson Controls
- **NEC**
- **Oi**
- Oosto (former Anyvision)
- RC International
- Security Team Network S.A
- Unión Eléctrica S.A.
- Unitech S.A
- **Verint***
- ZTE

- **Empresas que respondieron.**
- Empresas que no respondieron.

*** La respuesta de Verint solo informó que su "negocio de ciberseguridad ahora es una empresa pública independiente llamada Cognyte Software Ltd" [traducción propia]. Nos pusimos en contacto con personal de Cognyte, quien originalmente estuvo abierto a hablar, pero luego nunca confirmó una fecha.**

Los problemas subyacentes de las respuestas de las empresas

En las respuestas que recibimos, identificamos varios patrones recurrentes:

1. **Evasión de la responsabilidad mediante caracterizaciones incorrectas de los productos:**

   Cellebrite se rehusó a caracterizar sus productos como herramientas de vigilancia, describiéndolos como "soluciones de inteligencia digital" que se utilizan en investigaciones relacionadas con la aplicación de la ley. Si las empresas no reconocen que la vigilancia es un riesgo significativo de los servicios que ofrecen, no pueden llevar a cabo sus procesos de debida diligencia para identificar y prevenir el impacto en los derechos humanos, tal como lo requieren los PRNU.

   Mientras tanto, **IDEMIA** (antes, Morpho) negó la implementación de "cualquier tipo de tecnología de vigilancia en Argentina, Brasil o Ecuador". Dijeron que los sistemas que utiliza la empresa "en estos países tienen como fin el uso de datos biométricos para prácticas forenses", una afirmación que se contradice con la información que compartieron las autoridades.

   De hecho, las agencias de aplicación de la ley de Argentina comenzaron a utilizar productos de Morpho antes de 2010, y la empresa IDEMIA es responsable de instalar y establecer el Sistema de Identificación Dactilar Automática del Ministerio de Seguridad (AFIS). Actualmente, su tecnología se utiliza en diversas partes de Argentina, como en Campana, Luján, Balcarce, Córdoba, Chaco, y en numerosas ciudades de la Provincia de Buenos Aires.

   En definitiva, la respuesta de IDEMIA ignora el hecho de que las tecnologías que permiten el reconocimiento biométrico remoto *son* tecnologías de vigilancia y pueden tener impactos negativos en los derechos humanos, o contribuir con ello. La empresa eligió disputar datos específicos y malinterpretar nuestros descubrimientos, por ejemplo, al intentar aclarar que Morpho RapID utiliza huellas dactilares, cuando nuestros informes dicen lo mismo, y también son datos biométricos.

   En sus breves respuestas, ni Cellebrite ni IDEMIA mencionaron los derechos humanos, y mucho menos su responsabilidad corporativa de respetarlos. Esto representa directamente un incumplimiento del Principio 11 de los PRNU: "Las empresas deben respetar los derechos humanos. Eso significa que deben abstenerse de infringir los derechos humanos de terceros y hacer frente a las consecuencias negativas sobre los derechos humanos en las que tengan alguna participación".

2. **Desvío de la responsabilidad hacia otros agentes**

   Muchas de las empresas intentaron distanciarse de las acciones de sus socios. **Andeantrade**, una empresa proveedora de productos Hikvision, centró su respuesta en las adquisiciones públicas y no brindó información en cuanto a los perjuicios a los derechos humanos. Dado

que, aparentemente, vieron nuestra solicitud de información como un reclamo de responsabilidad, no proporcionaron información sobre los peligros para los derechos humanos y se basaron en el hecho de que son proveedores -no usuarios- de estas tecnologías, para distanciarse de cualquier impacto que los productos puedan causar.

La empresa brasilera **Intelbras** brindó respuestas detalladas a nuestras preguntas iniciales y de seguimiento. Si bien reiteraron la importancia de cumplir con las leyes de protección de datos personales, subestimaron la relevancia de la relación de su empresa con Dahua, la compañía China propietaria del 10% de sus acciones. Intelbras afirmó que "no tiene conexión ni responsabilidad por las acciones de la compañía China", pero dado que es accionista, un representante de Dahua forma parte de la junta directiva de Intelbras. Esto significa que Dahua tiene un grado de responsabilidad en garantizar que su inversión en Intelbras no contribuya a impactar negativamente los derechos humanos, al igual que Intelbras debe asegurarse de que los derechos humanos se respeten en todas sus operaciones comerciales.

La empresa brasilera **Oi** (antes, Telmar), así como **Intelbras**, argumentaron que los usuarios finales (sus clientes) son las únicas partes responsables del modo en que se utilizan sus productos o servicios. Mientras tanto, **Dahua** afirmó que "no pueden controlar completamente cómo [sus] tecnologías son utilizadas en última instancia por los usuarios finales". Esta narrativa ignora el hecho de que la responsabilidad corporativa se extiende por toda la cadena de valor de la empresa. Al respecto, el PRNU 13 (b) establece que las empresas "traten de prevenir o mitigar las consecuencias negativas sobre los derechos humanos directamente relacionadas con operaciones, productos o servicios prestados por sus relaciones comerciales, incluso cuando no hayan contribuido a generarlos".

A nivel operativo, los procesos de debida diligencia de las empresas deben considerar los impactos en los derechos humanos, no solo de sus productos, sino también de cualquier actividad relacionada (PRNU 17 (a)). Cuando las empresas no aceptan su responsabilidad por los daños que provocan las tecnologías que crean, limitan la capacidad de proteger la privacidad de las personas que sufren los efectos de las herramientas con capacidades de vigilancia.

3. Preocuparse por la clientela, pero no por las personas afectadas

La respuesta de **Oi** se centró en su desarrollo de productos y servicios alineados con la transformación digital y las tendencias de mercado, pero no hizo mención de cómo esta empresa protege los derechos humanos. Esto representa un incumplimiento del requisito de los PRNU que establece que las empresas deben comprometerse mediante sus políticas a respetar los derechos humanos (PRNU 15) y comunicar públicamente cómo abordan los impactos de sus productos o servicios en estos derechos (PRNU 21).

Intelbras proporcionó información sobre la asistencia previa y posterior a la venta que brinda a los clientes y las personas encargadas de la instalación, y sobre su compromiso con informar al "usuario y las autoridades competentes" si se produce un "incidente que afecte los datos personales de quienes utilizan sus servicios". No obstante, los verdaderos riesgos de las tecnologías con capacidades de vigilancia no las enfrentan los clientes que las implementan, sino las personas expuestas a tales tecnologías. El verdadero problema aquí es cómo las empresas limitarán a los clientes gubernamentales, en especial a aquellos con antecedentes de violaciones de derechos humanos. Aun así, Intelbras ignoró este aspecto en su respuesta, lo cual sugiere que esta empresa no evaluó el impacto de su negocio en los derechos humanos, tal como lo exige el PRNU 18.

4. Confianza excesiva en sus políticas internas a pesar de la falta de transparencia

En respuesta a nuestra pregunta sobre las políticas, los protocolos o los procesos internos que rigen el aprovisionamiento de soluciones de vigilancia a los gobiernos, varias empresas hicieron referencia a sus licencias y políticas de privacidad de datos, las condiciones de uso de los productos y los códigos de ética, así como a las reglamentaciones locales. Si bien las políticas internas son un punto de partida para el cumplimiento de las leyes, no son suficientes para garantizar la protección de los derechos humanos. Tal como lo indica el PRNU 16, "las empresas deben expresar su compromiso con el cumplimiento de esta responsabilidad".

Por ejemplo, **Oi** indicó que "operan en todos sus proyectos y operaciones observando los estándares más altos de gobernanza, integridad, ética corporativa y respeto por todas las regulaciones y leyes aplicables". Aun así, la empresa no hizo referencia a la implementación de estándares internacionales o de derechos humanos.

Cellebrite respondió a través de una agencia de relaciones públicas. Su respuesta breve describe los productos que vende y establece que la empresa cuenta con "estrictas políticas de licencia y restricciones para gobernar cómo los clientes utilizan [sus] soluciones, y solo vende[n] [su] tecnología a empresas, organizaciones y agencias que aceptan cumplir las estrictas políticas de licencias que rigen su uso correcto". Sin embargo, la empresa no brindó detalles sobre esas políticas, lo que impide que la sociedad civil supervise o verifique el cumplimiento de dichos compromisos.

IBM indicó que emplea "procesos rigurosos en todas sus operaciones globales para protegerse de las relaciones comerciales directas o indirectas que podrían perjudicar dichos compromisos". Si bien su respuesta completa establece compromisos claros alineados con los PRNU, por ejemplo, mediante el rechazo del uso de tecnologías de vigilancia masiva y perfilamiento racial, la empresa no brindó información sobre los procesos en sí, lo cual nos impide realizar un análisis completo y detallado.

NEC dio un paso más al crear los Principios de la IA y los derechos humanos del grupo NEC para "demostrar respeto por la privacidad y los derechos humanos en relación con la aplicación y la utilización de la IA y los datos biométricos en todas sus operaciones". No obstante, si bien el grupo evalúa si sus productos se utilizan para violar derechos humanos, la empresa no hizo mención de los canales que utiliza para reportar potenciales abusos ni brindó detalles sobre cómo se evalúan y se abordan los incumplimientos (PRNU 20). El respeto por los derechos humanos debe ir más allá de un grupo de trabajo o un estatuto de principios.

En resumen, en sus respuestas, las empresas hicieron referencia a políticas y principios internos, códigos de ética y grupos de trabajo, pero no brindaron detalles sobre los distintos mecanismos o información detallada sobre cómo se implementan o supervisan. (PRNU 20).

La transparencia exhaustiva, detallada y continua es fundamental para proteger los derechos humanos, en particular en las asociaciones público-privadas que permiten el despliegue de tecnologías de vigilancia. Los estados tienen la responsabilidad de proteger los derechos fundamentales, mientras que las empresas deben respetarlos. Por lo tanto, las empresas deben cumplir con los estándares de debida diligencia en cuanto a la transparencia y los derechos humanos, y deben brindar suficiente información para que la sociedad civil y otras entidades independientes controlen el cumplimiento de dichas responsabilidades.

Access Now

www.accessnow.org

Access Now defiende y extiende los derechos digitales de las personas y comunidades en riesgo. Como organización que va de la base a lo global, nos asociamos con actores locales para llevar la agenda de derechos humanos al uso, desarrollo y gobernanza de las tecnologías digitales, y para intervenir allí donde las tecnologías impactan negativamente en los derechos humanos. Al combinar el apoyo técnico directo, la incidencia estratégica, la concesión de subvenciones a actores de base, y convocatorias como RightsCon, luchamos por los derechos humanos en la era digital.

Para obtener más información, por favor contacte a:
Ángela Alarcón
Campaigner, Latin America & the Caribbean
angela@accessnow.org