Empresas y derechos humanos: informe regional sobre Tecnología, Big Data y Cibervigilancia

31 de mayo 2018

I. Introducción

El presente documento ha sido elaborado colectivamente para responder a algunas de las preguntas hechas por la Relatoría Especial sobre Derechos Económicos, Sociales, Culturales y Ambientales (REDESCA) de la Comisión Interamericana de Derechos Humanos (CIDH). En particular, queremos dar pistas sobre cómo las empresas que trabajan en el campo de la **tecnología, big data y cibervigilancia** responden o no a los marcos de derechos humanos en nuestro continente.

Internet y diversos medios electrónicos constituye actualmente una plataforma para el ejercicio de derechos humanos, incluyendo derechos civiles y políticos, pero también derechos económicos, sociales y culturales. El desarrollo de la tecnología en los últimos años ha contribuido particularmente a crear plataformas, productos y servicios que redundan en una mejor calidad de vida, mejor acceso a la educación, la cultura, la información, la libertad de expresión, los derechos de asociación y reunión, el derecho al trabajo, etc.

En esta industria, quizás como en ninguna otra, son las empresas quienes controlan el espacio de interacción y están situadas a lo largo de todas las capas de internet, recogiendo actividades que van desde la conexión (telecomunicaciones) hasta las plataformas de servicios (Google, Facebook, etc.), a lo que se suman empresas productoras de software, de seguridad digital, vigilancia, etc. Además, por la naturaleza abierta, global y descentralizada de internet , las empresas que trabajan en este medio no reconocen los límites territoriales tradicionales, pudiendo estar basadas en Estados Unidos (EE.UU.), en China, o en la Antártida y operar globalmente, sin perjuicio de que deban cumplir con las leyes de los lugares donde están registradas.

En este escenario tan particular, y tal como expresó Luis Fernando García de la Red en Defensa de los Derechos Digitales, R3D (México) en la audiencia temática sobre "Inteligencia digital, ciberseguridad y libertad de expresión",[1] las empresas de internet tienen una importante responsabilidad de respetar los derechos humanos en el entorno digital, sin importar la extraterritorialidad o multi-jurisdiccionalidad de sus actividades, pues las decisiones que toman pueden afectar derechos como la libertad de expresión, la privacidad "o incluso derechos económicos, sociales y culturales" de miles de millones de personas alrededor del mundo.[2]

Los servicios y productos generados por estas empresas -en consonancia con la creciente digitalización de nuestras sociedades- son usados por parte importante de los gobiernos, otras empresas y las personas. Este documento destaca, primariamente, algunas de las prácticas y políticas que directa o indirectamente constituyen un riesgo para los derechos humanos de todos los usuarios pero, particularmente, de sectores más vulnerables como son **periodistas**, **personas defensoras de derechos humanos, mujeres, pueblos indígenas, personas y comunidades afrodescendientes y población LGBTIQ**.

Para eso, y considerando el marco del cuestionario, nos concentramos en dos aspectos: big data y cibervigilancia.

- Big Data

[1] Audiencia pública ante la CIDH: visibilizando el impacto de las tecnologías digitales en los DDHH https://adcdigital.org.ar/2018/02/20/audiencia-publica-ante-la-cidh-visibilizando-impacto-las-tecnologias-digitales-los-ddhh/

[2] Audiencia hecha en el marco del 167 periodo de sesiones extraordinarias de la Comisión Interamericana de Derechos Humanos, que se celebró en febrero de este año en en Bogotá, Colombia https://www.youtube.com/watch?v=8_t8VCwAiKE&feature=youtu.be

Un estudio reciente de Frost & Sullivan llamado “Analysis of Big Data and Analytics Market in Latin America”, da cuenta que el mercado combinado de datos en Brasil, México y Colombia generó un "ingreso de U$ 538.3 millones en 2015 y se espera que alcance U$ 1,956.5 millones para el 2020 a una tasa de crecimiento anual compuesto (CAGR) de 29.4 por ciento ".[3] No es sorprendente la adopción veloz de los esquemas de explotación de big data en el continente, sobre todo por parte de las empresas. Como afirma un estudio al respecto de la ONG Derechos Digitales, “la adopción de técnicas de Big Data tiene la potencialidad de generar grandes beneficios sociales y mejorar la productividad de distintos sectores económicos, en áreas como el retail, la minería, la investigación y el marketing”.[4]

Sin embargo, la utilización del big data, sin la correlativa adopción de controles y equilibrios adecuados, puede vulnerar los derechos humanos de las personas. Al respecto, un estudio de la Fundación Karisma define tres campos potencialmente riesgosos:[5]

1) *Intimidad y protección de datos*: El derecho fundamental a la intimidad y a la protección de datos puede verse afectado por el big data de diversas formas, pues los resultados del análisis de datos pueden revelar información personal que corresponde a su espacio íntimo, sin necesidad ni proporcionalidad alguna. En este sentido, el riesgo más directo en este punto es el hecho de que la recopilación y análisis de toda clase de datos pueda dar a conocer aspectos de la esfera íntima de una persona como sus hábitos, preferencias o su círculo social y familiar.
2) *Anonimización de datos*: Las herramientas para garantizar que los datos analizados en el big data no estén directamente relacionados con una persona son insuficientes. Hasta la fecha, no existen mecanismos infalibles para la anonimización de la información. Es más, incluso cuando se anonimizan o agregan datos puede perderse parte de su utilidad, por lo cual parece haber una dicotomía entre intimidad y utilidad de los datos.
3) *Discriminación y transparencia*: Aunque está estrechamente relacionada con la violación al derecho a la intimidad y la protección de datos, el análisis y la toma de decisiones basada en ese metodología puede traer como consecuencia la discriminación de grupos particulares. Este riesgo proviene de dos factores: (i) decisiones automatizadas; y (ii) falta de transparencia en los algoritmos. Significa que mientras se siga sin saber la forma en que funcionan y la información que los alimenta, los casos de discriminación se seguirán presentando, pues no hay quién pueda hacer una auditoría de los algoritmos para encontrar fallas o mejorarlos.

En la región, diversas organizaciones de la sociedad civil han denunciado las potenciales violaciones a los derechos humanos. Uno de los casos es el análisis de crédito por parte de empresas financieras. De acuerdo con el periódico Valor Econômico,[6] el procesamiento de datos de crédito factura cerca de 3 mil millones de reales (aprox. 930 millones de dólares) al año en Brasil, y puede duplicar su tamaño en pocos años. De acuerdo a Coding Rights de Brasil, “para analizar la información financiera, social y de comportamiento, muchas entidades de crédito recurren a los data brokers, los corredores de datos, empresas que se dedican a recopilar, procesar y vender información personal sobre perfiles de consumidores. Los data brokers revisan fuentes gubernamentales, redes sociales, registros de otras empresas y cualquier rincón de internet donde pueda haber disponible información útil para montar bases de datos de información personal. Separadas, las informaciones recopiladas tienen poco valor, pero cuando se reúnen y organizan de acuerdo con ciertos patrones se vuelven más interesantes para las empresas que contratan esos servicios. La lista de clientes es amplia y abarca desde instituciones financieras y de seguros hasta empresas de telecomunicaciones, campañas electorales e incluso organismos gubernamentales”.[7] Para el Instituto Brasileño de Defensa del Consumidor (Idec), que

---

[3] Rising Use of Data Analytics for Enhancing Customer Experience Opens up Vast Growth Opportunities for Big Data in Latin America https://ww2.frost.com/news/press-releases/rising-use-data-analytics-enhancing-customer-experience-opens-vast-growth-opportunities-big-data-latin-america/

[4] Información financiera y discriminación laboral en Chile. Un caso de estudio sobre big data https://www.derechosdigitales.org/wp-content/uploads/big-data-informe.pdf

[5] Big Data: un aporte para la discusión de la política pública en Colombia https://karisma.org.co/big-data-un-aporte-para-la-discusion-de-la-politica-publica-en-colombia/

[6] Novo birô de crédito gera incômodo http://www.valor.com.br/financas/4766869/novo-biro-de-credito-gera-incomodo

[7] Te están stalkeando para darte un valor https://chupadados.codingrights.org/es/te-estan-stalkeando/

investiga la actuación de esas empresas y aboga por cambios en el sistema,[8] la crítica principal es la falta de transparencia: no está claro para el consumidor qué criterios se utilizan para la elaboración de su nota de crédito.

Asimismo, el tema del big data se hace particularmente sensible cuando se asocia a conceptos de "ciudades inteligentes"[9] y con la identificación biométrica de ciudadanos para acceder a servicios públicos[10], esto, porque no se puede elegir estar o no en las bases de datos, las que, además, muchas veces están a cargo de empresas internacionales (como IBM, Cisco, Microsoft, Google, etc.) que pasan a tener datos estratégicos de nuestros principales centros urbanos, a pesar incluso de que muchas de ellas no tienen mecanismos de rendición de cuentas en nuestros países.

En una nota más reciente, la explotación de grandes volúmenes de datos con fines electorales por parte de empresas privadas contratadas por diversos partidos políticos -destapada con el reciente escándalo entre Cambridge Analytica y Facebook-[11] también ha levantado las alarmas. Preocupa no solo por la supuesta presencia de esa empresa en nuestros países, sino también la actividad de compañías con los mismos fines[12] y los diversos efectos que tiene su uso de los datos de las personas, como la manipulación informativa y la clasificación de las personas en categorías sin ningún conocimiento ni menos consentimiento. A esto se agrega la falta de transparencia con la que operan sus algoritmos computacionales.[13] Esta discusión, por cierto, trasciende a Cambridge Analytica y ha puesto sobre la mesa la legalidad y ética de modelos de negocios sustentados en la explotación de datos de las personas, tan en boga gracias a las empresas de Silicon Valley.

Por último, los Estados de la región, en cuanto proveedores de servicios, crecientemente recurren al análisis de big data para la adopción de decisiones en materia de políticas públicas, que abarcan desde la persecución criminal a la asignación de beneficios sociales,[14] para lo cual contratan en muchas ocasiones empresas que proveen de la tecnología o realizan tales análisis. Existe un ámbito de responsabilidad clara de tales empresas en esta esfera, en el sentido que los servicios ofrecidos al Estado en esta materia consideren una evaluación de impacto de los mismos en el ejercicio de derechos humanos, incluyendo en ello la exigencia de transparencia a los ciudadanos en los procesos de adopción e implementación de tales servicios.

- **Cibervigilancia**

Conforme la tecnología avanza y nuestras sociedades se digitalizan, las herramientas de vigilancia se han hecho cada vez más ubicuas, lo que permite un mayor poder de vigilancia para aquellos que pueden adquirir y manejar esas tecnologías. Asimismo, las agendas de combate a las actividades terroristas, la delincuencia organizada y la ciberseguridad, fomentadas por una preocupante visión punitivista que habilitaría a las autoridades a desplegar todo su aparato represivo, sumada a una idéia de solucionismo tecnológico y una lógica del *robocop,*[15] han hecho florecer una pujante industria de

---

[8] Cadastro positivo e direitos dos consumidores https://idec.org.br/sites/default/files/arquivos/cadastro_positivo_e_direitos_dos_consumidores_0.pdf

[9] Tarjeta multifunción, un paso más hacia la ciudad inteligente https://antivigilancia.org/es/2016/03/tarjeta-multifuncion-un-paso-mas-hacia-la-ciudad-inteligente/

[10] Smart cities como estrategia discursiva: el caso brasileño https://antivigilancia.org/es/2016/03/smart-cities-como-estrategia-discursiva-el-caso-brasileno/

[11] The Influence Industry: The Global Business of Using Your Data in Elections https://ourdataourselves.tacticaltech.org/posts/influence-industry/

[12] Instagis: el “gran hermano” de las campañas políticas financiado por Corfo http://ciperchile.cl/2018/01/03/instagis-el-gran-hermano-de-las-campanas-politicas-financiado-por-corfo/

[13] Editorial: La explotación de datos en Internet con fines electorales en América Latina https://antivigilancia.org/es/2018/05/editorial-explotacion-de-datos-con-fines-electorales-latam/

[14] Un ejemplo es lo que ocurre en Argentina. "En Salta usan inteligencia artificial para prever embarazos adolescentes" https://www.clarin.com/sociedad/salta-usan-inteligencia-artificial-prever-embarazos-adolescentes_0_r10wlG6jf.html

[15] Megaeventos: Um Legado de Vigilancia https://legadovigilante.codingrights.org

vigilancia en el mundo.[16] Así, por ejemplo, vemos que todos los años en nuestros propios países esta industria organizan ferias millonarias para vender sus productos, tanto para el sector público como privado.[17]

Aunque representen una amenaza a la privacidad de los ciudadanos, poco se reporta sobre la eficiencia de estos aparatos respecto a la seguridad pública. Centros de operaciones conectando cámaras por toda la ciudad, como el COR y el CICC desarrollados en Río de Janeiro en preparación para megaeventos como la Copa del Mundo y las Olimpíadas,[18] o el COT de la municipalidad de Tigre, en Argentina, más parecen funcionar como herramientas de propaganda política que instrumentos de seguridad pública.[19] Lo mismo ha pasado con el gobierno del estado de São Paulo, en Brasil, donde se gastó más de 10 millones de dólares en el sistema Detecta, de Microsoft, con "cámaras inteligentes" que, teóricamente, serían capaces de detectar actividades sospechosas, pero que nunca funcionaran más allá de instrumentos de filmación.[20]

Asimismo, el uso de productos y de servicios de cibervigilancia -vendidos por empresas privadas a los gobiernos del continente- para ser usados ilegalmente en contra de estos sectores de la población, tiene muchos ejemplos en el continente.[21] Uno de los más importantes es el reciente caso de México, donde existen fuentes fidedignas que dan cuenta del espionaje ilegal en contra de varias personas defensoras de derechos humanos, periodistas y activistas anti-corrupción. Las investigaciones hechas por la sociedad civil[22] así como por el laboratorio interdisciplinario de la Universidad de Toronto, Citizen Lab, han demostrado la utilización presuntamente por parte de autoridades mexicanas de un malware conocido como Pegasus, comercializado por parte de la empresa israelí NSO Group exclusivamente a autoridades gubernamentales, con la finalidad de espiar los teléfonos móviles de estas personas. El software malicioso funciona a través del envío de mensajes de texto que contienen enlaces infecciosos que permiten a Pegasus acceder a toda la información guardada en el dispositivo, la localización geográfica del mismo así como a la activación inadvertida del micrófono y la cámara. No obstante, y a pesar de la magnitud del caso, la investigación permanece en la impunidad.

La empresa NSO Group no es la única empresa de software de vigilancia con clientes en la región; conocido es el caso de la empresa italiana Hacking Team, que sabemos hasta ahora tiene presencia o inició negociaciones con sectores de los gobiernos de Brasil, Chile, Colombia, Ecuador, Honduras, México y Panamá, y la cual vende un software de naturaleza tan invasiva que, de acuerdo a la ONG Derechos Digitales, “tiene acceso a todo, incluyendo a las comunicaciones especialmente protegidas, sin que existan mecanismos adecuados para controlarlo”.[23]

A lo anterior, se suma el antecedente aportado por el informe de la Relatoría Especial sobre la situación de los defensores de los derechos humanos de la ONU, hecho en el 2016, y que reconoce que antes de ser asesinados, las y los defensores han sido víctimas de una serie de agresiones que incluyen,

---

[16] Privacy International launches the Surveillance Industry Index & New Accompanying Report. 2017. Privacy International. https://privacyinternational.org/blog/54/privacy-international-launches-surveillance-industry-index-new-accompanying-report

[17] Com a Copa, Brasil vira mercado prioritário da vigilância https://apublica.org/2013/09/copa-brasil-vira-mercado-prioritario-da-vigilancia/

[18] Megaeventos: Um Legado de Vigilancia https://legadovigilante.codingrights.org

[19] Vigilar y entretener, un modelo de negocios feliz https://chupadados.codingrights.org/es/vigiar-e-entreter-um-modelo-de-negocios-feliz/

[20] Alckmin vai relançar sistema que já custou R$ 30 milhões e não funciona http://www1.folha.uol.com.br/cotidiano/2017/06/1897306-alckmin-vai-relancar-sistema-que-ja-custou-r-30-milhoes-e-nao-funciona.shtml

[21] Recomendaciones para la transparencia y anticorrupción en la adquisición y uso de tecnologías de vigilancia por parte de los Estados americanos https://es.scribd.com/document/376302045/Recomendaciones-Para-La-Transparencia-y-Anticorrupcion-en-La-Compra-y-Uso-de-Tecnologias-de-Vigilancia-Por-Parte-de-Los-Estados-Americanos

[22] Citizen Lab, ARTICLE19 Oficina para México y Centroamérica, R3D: Red en Defensa de los Derechos Digitales y SocialTIC.

[23] Hacking Team: malware para la vigilancia en América Latina https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

entre muchas otras, la vigilancia ilícita.[24] Este es el caso, por ejemplo, en Brasil, donde en el 2013 se denunció que la minera transnacional Vale usaba métodos de espionaje a los movimientos sociales, interceptaciones telefónicas y revisiones en cajones y computadoras de sus empleados.[25]

El uso discriminatorio de la cibervigilancia es también preocupante. En Río de Janeiro, que actualmente se encuentra situación de intervención militar, ciudadanos habitantes de favelas tienen su derecho a desplazarse libremente intervenido por el establecimiento de "checkpoints" donde militares les obligaban a sacar fotos con sus registros de identidad para, al enviar la imagen por una aplicación, cruzar la información con una base de datos policial,[26] en clara violación al derecho a la presunción de inocencia. Los ejemplos de usos discriminatorios[27] de globos de vigilancia y drones[28] también tienen una muestra clara (y han producido amplia polémica pública) en países como Chile.

En esta materia cabe una responsabilidad clara de las empresas en cuanto proveedoras de tecnologías que son utilizadas para la cibervigilancia. Al ser proveedoras de tecnología que en sí misma tiene una alta potencialidad de afectación del ejercicio de derechos humanos de las personas, de ello se sigue que la vinculación con Estados demandantes de la misma o de terceros debe involucrar de parte de las empresas proveedoras una debida diligencia del contexto en que tales tecnologías pretenden ser utilizadas, que debe incluir la revisión de marcos legales que faculten y fijen las condiciones de su utilización lícita, y consideren las salvaguardias de debido proceso y transparencia que resulten compatibles con el respeto de los derechos humanos.

Asimismo, y tal como ocurre en la adquisición de otros productos o servicios por parte de los Estados, existe una responsabilidad de las empresas en cuanto a aportar a la transparencia de los procesos de adquisición de las misma, manteniéndose alejadas de prácticas que inciten a la corrupción de los órganos a cargo de tales adquisiciones,[29] y proporcionando información veraz y suficiente acerca de las limitaciones de las tecnologías ofrecidas en términos de seguridad, así como de eficacia para la persecución de los fines que el Estado invoca para su adquisición.

II. Cuestionario

a) Bloque 1: Información de Contexto

3. Emitir observaciones y comentarios sobre las obligaciones y estándares jurídicos internacionales, en particular aquellos provenientes del Sistema Interamericano de Derechos Humanos, que considera aplicables a los Estados miembros de la OEA en cada una de las situaciones identificadas en la pregunta 2.

En materia de tecnología, big data y cibervigilancia, existe un cúmulo de derechos humanos, tanto civiles y políticos, como económicos, sociales y culturales, que se ven impactados por la acción de las empresas y los Estados.

---

[24] Situación de los defensores de los derechos humanos https://digitallibrary.un.org/record/840291/files/A_71_281-ES.pdf
[25] Grave denuncia en contra de la transnacional minera Vale expone sus métodos de espionaje http://ciperchile.cl/2013/09/27/grave-denuncia-en-contra-de-la-transnacional-minera-vale-expone-sus-metodos-de-espionaje/
[26] Militares tiram fotos de moradores de favelas do Rio e de seus documentos https://g1.globo.com/rj/rio-de-janeiro/noticia/militares-tiram-fotos-de-moradores-de-favelas-do-rio-para-checar-antecedentes.ghtml
[27] Militarización en la Araucanía: Drones, aviones no tripulados y más de mil policías desplegados http://www.eldesconcierto.cl/2016/03/23/militarizacion-en-la-araucania-drones-aviones-no-tripulados-y-mas-de-mil-policias-desplegados/
[28] Drones en Chile: Un análisis de los discursos, industria y los derechos humanos. https://datosprotegidos.org/wp-content/uploads/2017/04/Informe-Drones-espa%C3%B1ol.pdf
[29] Recomendaciones para la transparencia y anticorrupción en la adquisición y uso de tecnologías de vigilancia por parte de los Estados americanos https://www.derechosdigitales.org/wp-content/uploads/Recomendaciones-para-la-transparencia-y-anticorrupcion-en-la-compra-y-uso-de-tecnologias-de-vigilancia-por-parte-de-los-Estados-americanos.pdf

En lo que se refiere a la implementación del uso de la tecnología en la vida cotidiana, hasta ahora el vínculo más directo al cual se ha intentado asociar es al impacto en el ejercicio de derechos civiles y políticos como lo son los de privacidad, libertad de expresión, pensamiento, opinión y asociación.

En tal sentido, el concepto de privacidad está consagrado en el derecho internacional, se basa en los conceptos fundamentales del honor personal y la dignidad. Hay disposiciones relativas a la protección de la privacidad, el honor personal y la dignidad en los principales sistemas de derechos humanos del mundo. Ello no resulta casualidad, pues de alguna forma el derecho a la privacidad resulta esencial para habilitar el ejercicio de otros derechos: nos comportamos con menor libertad cuando sabemos que nuestras acciones pueden encontrarse siendo observadas; este derecho es particularmente más relevante en contextos hostiles de inseguridad pública, corrupción o falta de estabilidad democrática.

En las Américas, estos conceptos están claramente establecidos en el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre (1948), donde se dispone el derecho a la protección a la honra, la reputación personal y la vida privada y familiar: "Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar". Estos conceptos también se establecen en los artículos 11 y 13 de la Convención Americana sobre Derechos Humanos ("Pacto de San José") (1969) (apéndice A). Así, por ejemplo, en su Artículo 11 la protección de la honra, dignidad y vida privada en los siguientes términos: "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

La Corte Interamericana de Derechos Humanos ha confirmado el derecho a la privacidad en su sentido más tradicional, donde el derecho a la vida privada implica una obligación negativa para el Estado. "[E]l ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública".[30]

Además, la constitución y las leyes fundamentales de muchos Estados Miembros de la OEA garantizan el respeto y la protección de la privacidad, la dignidad personal y el honor familiar, la inviolabilidad del hogar y las comunicaciones privadas, los datos personales y conceptos conexos. Casi todos los Estados Miembros de la OEA han adoptado algún tipo de ley con respecto a la protección de la privacidad y los datos (aunque sus disposiciones varían considerablemente en lo que se refiere a su enfoque, ámbito de aplicación y contenido).

Efectivamente, América Latina en general ha adoptado mayormente durante la década de 1990 leyes comprensivas para el procesamiento de datos personales, es decir, leyes que regulan el procesamiento automático y manual de datos personales tanto por el sector público como por el sector privado. De tal suerte ha seguido también la tradición europea de protección comprensiva, a diferencia por ejemplo de los Estados Unidos, cuya protección es fragmentada por sector y se basa, muy sucintamente, en criterios de privacidad y datos de alta sensibilidad, no en la autodeterminación informativa.[31]

A propósito de su informe sobre "Libertad de Expresión en Internet" del 2013, la Relatoría Especial para la Libertad de Expresión de la CIDH, ha manifestado que "(l)a protección del derecho a la vida privada implica al menos dos políticas concretas vinculadas al ejercicio del derecho a la libertad de pensamiento y expresión: la protección del discurso anónimo y la protección de los datos personales", y además recuerda que "los Estados están obligados a prohibir el uso de los datos personales para fines contrarios a los tratados de derechos humanos y a establecer derechos de información, corrección y —de ser necesario y proporcionado— eliminación de datos, así como a crear mecanismos de supervisión efectivos".[32]

También reconoce que la vigilancia masiva de las comunicaciones cibernéticas, en sí "una injerencia en la privacidad de las personas", debe, por ello, someterse a las condiciones antes identificadas

---

[30] Caso de las Masacres de Ituango vs. Colombia, Sentencia de 1 de julio de 2006 (párr. 149) http://www.corteidh.or.cr/docs/casos/articulos/seriec_148_esp.pdf
[31] Desafíos en el debate de la protección de datos para Latinoamérica https://www.consejotransparencia.cl/wp-content/uploads/2018/04/v_milanes__1_.pdf
[32] Libertad de expresión en Internet https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf

(legalidad, persecución de un fin legítimo, racionalidad medio-fin, necesidad, excepcionalidad, carácter taxativo y estricto de las autorizaciones).[33]

En lo que toca a los derechos económicos, sociales y culturales, el Sistema Interamericano nace dándoles reconocimiento a través de la Declaración Americana de los Derechos y Deberes del Hombre, sin embargo, su más amplio reconocimiento y especificación emana a nivel internacional del Pacto Internacional de Derechos Económicos de las Naciones Unidas, Sociales y Culturales, que entró en vigencia el 3 de enero de 1976, que tiene su correlato en el Sistema Interamericano en el Protocolo Adicional a la Convención Americana sobre Derechos Humanos en materia de Derechos Económicos, Sociales y Culturales o "Protocolo de San Salvador". Todos estos instrumentos abarcan el derecho al trabajo, a beneficiarse de la cultura, a la salud, a la seguridad social y a la educación.

En un sentido más amplio, la tecnología, y en particular internet, son en la actualidad recursos prácticamente imprescindibles para posibilitar el ejercicio de derechos económicos, sociales y culturales. Los Estados se valen de la tecnología para proveer acceso a la educación, servicios de salud, seguridad social, proveer empleo y facilitar el acceso a la cultura, entre otros. En la publicación de 2106 de Association for Progressive Communications titulada “Global Information Society Watch 2016” (GISWATCH)[34] se identificaron algunos ejemplos que ilustran la relación entre internet y los derechos económicos sociales y culturales en nuestra región:

- En situaciones en las que determinados procesos y servicios del gobierno se pueden llevar a cabo solamente en línea y en el idioma predominante, las condiciones de discriminación se agravan para determinados grupos poblacionales. Ese es el caso de los mecanismos para acceder a los servicios sociales en Argentina por parte de poblaciones indígena.
- En Perú, el proyecto Mapa Sonoro, de fonética en línea, apunta a desafiar la exclusión estructural indígena otorgándole visibilidad a lenguajes indígenas marginalizados con propósitos educacionales y de acceso al conocimiento.
- El teletrabajo se ha tornado en una alternativa ventajosa de trabajo, pero si no se encuentra reglamentado puede dar lugar a explotación laboral, como es el caso de Panamá.
- En el caso de Venezuela, internet es usada intensivamente por la población para paliar la falta de alimentos y medicinas. Mediante redes sociales, la población organiza trueques. El Gobierno, que ha negado la crisis, configuró un sistema centralizado de base de datos biométricos enlazando a supermercados y farmacias con el propósito de monitorear y controlar el suministro y la compra de productos.
- A pesar de los obstáculos que ha enfrentado, el programa Ceibal en Uruguay ha logrado conectar a más del 50% de la población de escasos recursos a internet. Se trata de un ejemplo de cómo las iniciativas de educación en línea pueden usarse para habilitar derechos socio-económicos de las comunidades y cómo las políticas de educación contribuyen a la inclusión social.
- El establecimiento de hubs tecnológicos rurales en Costa Rica ha mostrado tener valor para el empoderamiento social y económico de las mujeres rurales en el país.

Garantizar un mayor acceso a internet por parte de los Estados se vuelve una necesidad como parte del cumplimiento de su obligación de garantizar el ejercicio de derechos económicos, sociales y culturales, sin que dicha obligación se agote en la mera posibilidad de conexión a la red, sino que abarca el que tal conexión goce de características de costos, estabilidad y accesibilidad que permita que internet sea usado como una herramienta eficiente para el acceso al empleo, la salud, los servicios de seguridad social, y la cultura, entre otros. No basta entonces con la mera digitalización o tecnologización de servicios de los Estados a través de creación de plataformas de servicios en línea, tales servicios deben encontrarse disponibles en lenguajes y formatos accesibles para proveer acceso efectivo por diferentes sectores de la población, particularmente aquellos en situación más vulnerable por condiciones de discapacidad, analfabetismo, género, ubicación geográfica, pertenencia a etnias o grupos minoritarios, o incluso por edad. La eficiencia que se busca por los Estados a través de la implementación de tecnología en el cumplimiento de sus obligaciones de promover el ejercicio de derechos económicos y sociales debe tener en consideración mecanismos alternativos de ejercicio de

[33] Libertad de expresión en Internet https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf
[34] Ver http://www.giswatch.org. Todos los ejemplos mencionados a continuación se encuentran en el reporte 2016.

tales derechos que sean consistentes con no marginar a segmentos de su población de su pleno disfrute. Cabe a este respecto una responsabilidad social de las empresas promotoras y muchas veces proveedoras de tales sistemas, que tienen la obligación de explicitar las limitaciones de los mismos a la hora de ofrecerlos a los Estados, así como comprometer la búsqueda de soluciones (no siempre tecnológicas) que permitan hacerse cargo de las limitaciones de los sistemas tecnológicos que ofrecen. Algunas de estas empresas han avanzado al desarrollo de principios en la labor de implementación de proyectos de Innovación pública, Gobierno Digital, Gobierno Abierto y Ciudades Inteligentes, pero en general ellos carecen de una aproximación de derechos humanos.[35]

Particularmente, las tecnologías de big data y cibervigilancia impactan sobre el ejercicio de todos los derechos recién enunciados, en la medida que a través de dichas soluciones tecnológicas se permite obtener un perfil completo de los comportamientos de las personas en cada una de las esferas en que ellas se manifiestan, y permiten a las empresas en control de tales tecnologías, la toma de decisiones que impactan en las posibilidades de empleo, acceso a la cultura, acceso a cobertura de salud, acceso a beneficios sociales y acceso a la educación de las personas. Ello porque la recogida masiva de información permite una discriminación cada vez más perfecta entre individuos, ya sean ellos trabajadores, clientes o simples ciudadanos a los que las empresas apuntan sus servicios, directamente o como delegadas del ejercicio de funciones públicas. Tanto en lo que respecta al ejercicio de derechos civiles y políticos, como económicos, sociales y culturales, aquello que facilitan tecnologías como el uso de big data y herramientas de cibervigilancia es un ejercicio perfecto de acciones de discriminación a cuya erradicación se han comprometido los Estados Americanos en la Convención Interamericana contra toda forma de Discriminación e Intolerancia.

Muchos de los servicios del Estado han sido tercerizados a través de empresas que los proveen, con lo cual existe una responsabilidad directa de los Estados y de las empresas que ejercen esa función delegada de cautelar que el uso de dicha tecnología mire en todos los casos al más pleno ejercicio de tales derechos, pero siempre en concordancia con el respeto de otros derechos humanos involucrados. No es posible que en nombre de una mayor eficiencia en la distribución de servicios por parte de los Estados se vulnere la dignidad y derechos civiles y políticos de las personas receptoras de tales servicios.[36] Por tanto, corresponde que las empresas productoras de tales tecnologías, que se sirven de aquellas para el desarrollo de sus negocios, así como los Estados en que ellas desarrollan sus actividades, asuman la responsabilidad por el uso de tales herramientas en una forma consistente con el respeto de las diferentes categorías de derechos aquí enunciadas en consistencia a los instrumentos internacionales y del Sistema Interamericano que los reconocen y cautelan.

Por último, la responsabilidad de las empresas que ha sido aquí establecida tiene como fuente directa en el sistema internacional los Principios Rectores sobre las empresas y los derechos humanos de las Naciones Unidas, que fueron elaborados por el Representante Especial del Secretario General para la cuestión de los derechos humanos y las empresas transnacionales y otras empresas, y que fueron aprobados por el Consejo de Derechos Humanos en su resolución 17/4, de 16 de junio de 2011 (en adelante, Principios Rectores).

b) Bloque 2: Marcos Normativos y Políticas Públicas

4. Suministrar información sobre marcos normativos (v.g. legislación, reglamentos, etc) y políticas públicas (v.g. Planes de Acción Nacional) sobre empresas y derechos humanos. Identifique y proporcione aquellas normas y políticas vigentes relacionadas con la materia.

En términos generales, el debate en torno al desarrollo de políticas públicas de los Estados en nuestra región para la implementación y masificación del uso de tecnologías ha carecido de un enfoque de desarrollo sustentable, que ponga el énfasis no solo en la efectividad de la tecnología para impulsar el crecimiento económico, sino también cómo la implementación de tal tecnología se hace cargo de garantizar el más pleno ejercicio de los derechos de las personas en la región, determinando así una

[35] Un ejemplo puede verse aquí https://asimov.cl/site/templates/assets/files/Cuadernos-eGob-3-Principios-Gob-Digital.pdf
[36] Biometría: tecnosolucionismo a costa de nuestros derechos https://www.derechosdigitales.org/11333/biometria-tecnosolucionismo-a-costa-de-nuestros-derechos/

más equitativa participación de los beneficios que el crecimiento económico asociado al uso de la tecnología implica.

Lo anterior, requiere de una evaluación del impacto en el ejercicio de derechos humanos (tanto civiles y políticos, como económicos y sociales) de una determinada política pública orientada al desarrollo o implementación de tecnología, tanto al momento de su diseño, como en su fase de implementación. Cuestión que se encuentra ausente sistemáticamente de las políticas públicas promovidas en materia de tecnología en la región.[37]

En particular, los marcos normativos y de políticas públicas respecto a la tecnología, big data y cibervigilancia que busquen alentar prácticas empresariales en el marco de los derechos humanos son más bien nulos (con la excepción de situaciones puntuales como el caso colombiano, que se discutirá más adelante en esta respuesta). No obstante, nos parece importante señalar que sí existen instancias generales que debiesen obligar al sector privado a adecuar sus prácticas al respeto de los derechos humanos.

- Protección de datos personales

En la era de la digitalización, la protección de nuestros datos personales y privacidad son fundamentales. Las empresas que trabajan relacionadas con la tecnología deben adecuarse a las normativas locales en donde despliegan sus servicios, y donde ellas no existan, a los estándares internacionales de respeto y protección de los derechos humanos, que como hemos señalado más arriba, recogen el respeto a la privacidad y otros derechos cuyo ejercicio se involucra en el tratamiento de datos personales.

Así, la protección de las personas en relación con el tratamiento de sus datos personales es un derecho fundamental que se encuentra reconocido con rango máximo en la mayoría de las Constituciones Políticas de los Estados del continente, bajo la forma del derecho a la privacidad o a la protección de datos personales a través del recurso habeas data, y en otros casos ha sido definido jurisprudencialmente por sus Tribunales o Cortes Constitucionales.

América Latina, en general, durante la década de los 90 adoptó leyes comprensivas para el procesamiento de datos personales, es decir, leyes que regulan el procesamiento automático y manual de datos personales tanto por el sector público como por el sector privado. De acuerdo a Valeria Milanes de ADC Argentina, países en el continente han “seguido también la tradición europea de protección comprensiva, a diferencia por ejemplo de los Estados Unidos, cuya protección es fragmentada por sector y se basa, muy sucintamente, en criterios de privacidad y datos de alta sensibilidad, no en la autodeterminación informativa”.[38] Actualmente, muchos países se encuentran en un estado de transición, donde o se están empujando por primera vez leyes generales de protección de datos (el caso de Brasil es el más paradigmático), o se trabaja para su actualización (como en Argentina o Chile, por ejemplo).

El rol que cabe a las empresas a este respecto es el de abstenerse de utilizar su capacidad económica para influir en la definición de los marcos normativos que se adopten sean limitados o, en algún sentido, contrarios al más pleno ejercicio de los derechos humanos antes identificados. En un contexto global de desarrollo de negocios ligados a la tecnología, resultaría esperable que los más altos estándares internacionales con que las empresas ya operan en otras jurisdicciones en que tales se han implementado, como es el caso de Europa con el GDPR,[39] sean ofrecidos también en nuestra región en la cual las mismas empresas prestan servicios.

- Explotación de big data

Desde abril del 2018, Colombia cuenta con el documento CONPES 3920 que define la política de explotación de datos (Big Data) para el Estado colombiano. Con este documento, el país asume el

---

[37] Las ciudades inteligentes y el problema de la vigilancia https://www.derechosdigitales.org/10720/las-ciudades-inteligentes-y-el-problema-de-la-vigilancia/
[38] Desafíos en el debate de la protección de datos para Latinoamérica https://www.consejotransparencia.cl/wp-content/uploads/2018/04/v_milanes__1_.pdf
[39] Why and how GDPR applies to people globally https://www.privacyinternational.org/feature/2054/why-and-how-gdpr-applies-people-globally

liderazgo regional al ser el primero en Latinoamérica, y octavo en el mundo, con una política pública integral que habilita el aprovechamiento de los datos para generar desarrollo social y económico. En el texto se reconoce como un riesgo que debe ser tenido en cuenta "el hecho de que el análisis de datos puede llevar a la toma de decisiones erróneas, debido a sesgos que no hayan sido contemplados o eliminados de los datos empleados. Por ejemplo, una herramienta usada para determinar la probabilidad de comisión de delitos y reincidencia puede presentar resultados errados porque los datos contenían un sesgo racial que no fue identificado y eliminado. Así mismo, los datos pueden ser empleados de manera indebida en contextos de transacciones privadas, por ejemplo, para imponer tasas más altas en la venta de seguros a partir de la revisión del historial de navegación en Internet, limitar la capacidad de decisión mediante la exposición limitada de contenido, o el aumento de precios de acuerdo con los patrones de consumo, entre otros".

Para eso define tareas para que en los próximos años se avance en las necesarias actualizaciones en la protección de datos personales y derechos asociados a estos (privacidad e intimidad). Asimismo, habla de establecer lineamientos que deben aplicar las entidades públicas para el adecuado tratamiento de los datos personales de los ciudadanos, alineados con el principio de responsabilidad demostrada, "desarrollado en la reglamentación e incorporando la privacidad por diseño y defecto de los datos personales. De esta manera, se busca superar el cumplimiento de mínimos y convertir la gestión de los datos en una actividad rutinaria que garantice la protección de los datos personales de los ciudadanos".

Además, habla de levantar mesas (en las que estén representantes del sector público, privado, la academia, la sociedad civil y los ciudadanos) que identifiquen e incorporen buenas prácticas y esquemas de autorregulación exitosos para definir el marco ético para la explotación de datos en el país: "El consenso ético se formalizará en un compromiso de todos los actores mencionados para la implementación de prácticas de autorregulación, de modo que, además de las previsiones jurídicas se cuente con un consenso social respecto del uso de los datos para la generación de valor económico y social, sin afectar las garantías de los ciudadanos o generar algún detrimento en los derechos reconocidos y protegidos por el marco jurídico".

Por su parte en Chile, el Estado ha implementado el portal www.datos.gob.cl que contiene la información de servicios y organismos públicos, con el objetivo de proveer a las personas y empresas acceso a la información en base a la cual el gobierno toma decisiones para las políticas públicas. La información así disponible puede ser utilizada para el desarrollo de investigaciones, construcción de aplicaciones y conducción de análisis de diversa índole. En la actualidad, la información disponible abarca a más de 1000 sets de datos de 521 organizaciones públicas. Lo anterior forma parte de la política de datos abiertos impulsada por el Instructivo Presidencial N°5 del 12 de noviembre de 2012,[40] donde se llama a todas las instituciones gubernamentales, a publicar datos en formatos abiertos y reutilizables, en cumplimiento del compromiso adoptado por el Estado Chileno como parte del primer plan de acción de Chile ante el Open Government Partnership.

- Planes nacionales de ciberseguridad

El "Informe Ciberseguridad 2016, ¿Estamos preparados en América Latina y el Caribe?",[41] hecho por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA), reveló que cuatro de cada cinco países de la región no tenía estrategias de ciberseguridad o planes de protección de infraestructura crítica. Dos de cada tres no cuentan con un centro de comando y control de seguridad cibernética. La gran mayoría de las fiscalías carece de capacidad para perseguir los delitos cibernéticos, entre otras carencias.

En este contexto, la OEA misma ha impulsado a los países de la región a que adopten planes de ciberseguridad, y ha recomendado a los países a desarrollarlos de manera consistente con los derechos humanos y los valores fundamentales reconocidos en sus constituciones. Los planes de ciberseguridad pueden tener un efecto en las empresas, en tanto sus actividades están entre las principales afectadas por ataques cibernéticos, además de ser muchas veces los prestadores de servicios digitales y productos de ciberseguridad a los Estados.

[40] Disponible en: http://www.gobiernoabierto.gob.cl/sites/default/files/gab.pres.ndeg005.pdf
[41] Ciberseguridad en América Latina y el Caribe: ¿Estamos preparados?https://digital-iadb.leadpages.co/ciberseguridad-en-la-region/

En la actualidad Colombia[42], Costa Rica[43], Chile[44], México[45], Panamá[46] y Paraguay[47] cuentan con políticas, planes o estrategias nacionales de ciberseguridad aprobadas y en fase implementación, mientras en países como Argentina, Brasil, Guatemala y Perú, ellas se encuentran en diferentes fases de elaboración y discusión.

Ninguno de tales planes resulta específico en abordar la regulación de las capacidades de cibervigilancia de los Estados o su relación con la provisión de tales servicios por parte de las empresas. Sin embargo, todos ellos contienen, con diferente énfasis, la manifestación de un compromiso de enfoque de derechos en materias que atañen a la ciberseguridad, compromiso contra el cual las acciones de los Estados y de las empresas pueden ser medidos en materia de implementación de servicios de cibervigilancia.

- Empresas y derechos humanos

Existen iniciativas nacionales que buscan implementar los Principios Rectores de Naciones Unidas. Aunque aún no abordan las actividades empresariales relacionadas con la tecnología, el big data o la cibervigilancia, vemos un camino posible para aprovechar el trabajo que tanto a nivel internacional como nacional se ha hecho para promover la protección, respeto y reparación de prácticas empresariales de, por ejemplo, la industria extractivista.

Colombia, desde 2014, cuenta con un marco orientador de la acción del Estado para garantizar el goce efectivo de los derechos humanos y su respeto por parte de las empresas. Con ello, el gobierno colombiano ha querido generar una estructura que permita abordar los riesgos mediante una "adecuada organización del Estado, una claridad normativa y unos mecanismos de remediación". Las recomendaciones que recoge este documento cubren (1) búsqueda de compromisos entre los sectores públicos, privados y sociales; (2) difusión y pedagogía de los mecanismos de denuncia y acciones de remediación; (3) la generación de incentivos; (4) la armonización de políticas; y (5) el desarrollo de indicadores para medir y evaluar los logros.

Esta política está estructurada en torno a los 3 pilares reconocidos en los Principios Rectores, a saber: (1) el deber del Estado de proteger los derechos humanos; (2) la responsabilidad de las empresas de respetar los derechos humanos y (3) el acceso efectivo a mecanismo de reparación.

A un año de la formulación del anterior texto, el Gobierno colombiano adoptó el Plan Nacional de Acción en Derechos Humanos y Empresa, una política orientada a armonizar "la protección y garantías de los derechos humanos y el desarrollo económico". Esta política prioriza 3 sectores – minero-energético, agroindustria e infraestructura vial– con alto potencial para generar conflictividad social. Este plan fue diseñado a tres años, por lo que es de esperarse que entre 2018 y 2019 se revise y se formule una política que dé continuidad al compromiso asumido por el Estado de proteger los derechos humanos en relación con las actividades empresariales. Además, es una oportunidad para incluir un nuevo sector económico que cada vez más tiene impactos en los derechos de las personas: el tecnológico.

---

[42] POLITICA NACIONAL DE SEGURIDAD DIGITAL https://www.mintic.gov.co/portal/604/articles-14481_recurso_1.pdf
[43] Estrategia Nacional de Ciberseguridad de Costa Rica https://micit.go.cr/images/imagenes_noticias/10-11-2017__Ciberseguridad/Estrategia-Nacional-de-Ciberseguridad-de-Costa-Rica-11-10-17.pdf
[44] Política Nacional de Ciberseguridad http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf
[45] Estrategia Nacional de Ciberseguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
[46] Gaceta Oficial Digital, viernes 17 de mayo de 2013 https://www.unodc.org/res/cld/lessons-learned/pan/estrategia_nacional_de_seguridad_cibernetica_y_proteccion_de_infraestructuras_criticas_html/Estrategia_Nacional_de_Seguridad_Cibernetica_y_Proteccion_de_Infraestructuras_Criticas.pdf
[47] Plan nacional de ciberseguridad https://www.senatics.gov.py/plan-nacional-de-ciberseguridad

Por su parte, en 2017 Chile dictó su primer Plan de Acción Nacional en Derechos Humanos y Empresas que tendrá una vigencia de 3 años hasta 2019. Este plan se manifiesta como la materialización del compromiso asumido por el Estado chileno con la Agenda 2030 para el Desarrollo Sostenible, para terminar con la pobreza, reducir la desigualdad y luchar contra el cambio climático. Dicha agenda reconoce el rol de las empresas y destaca la necesidad de un trabajo conjunto, público-privado, para lograr estos objetivos. De acuerdo a lo enunciado en éste, el plan busca aportar claridad respecto a lo que se entiende por derechos humanos en el ámbito empresarial y constituye, además, una plataforma para identificar, prevenir, abordar, mitigar y reparar los impactos adversos que pueden generar las empresas al realizar sus actividades.

Tal como se describe en el plan, éste tiene como objetivo principal instalar en Chile una cultura de respeto de los derechos humanos en la actividad empresarial con el fin de prevenir los impactos negativos y, de ser posible, ir más allá del respeto, potenciando los aportes positivos que las empresas pueden dar a la sociedad y su entorno. Se reconoce directamente en éste que de acuerdo a la Declaración Universal de Derechos Humanos, tanto las personas como las instituciones deben promover y respetar los derechos humanos.

El plan de acción se conforma en base a los compromisos de diversas instituciones del Estado, el cual actúa bajo la responsabilidad que le cabe en materia de protección de derechos humanos. En la preparación del plan el Estado convocó a terceros, entre ellos a las empresas, con el fin de que aportaran al proceso de elaboración. También existe la expectativa de que diversos actores sociales participen en su implementación, monitoreo y seguimiento.

No existe mención explícita en el plan al área de provisión de tecnología o servicios tecnológicos por las empresas, pero en el pilar Nº2 que recoge las expectativas del Estado en materia de responsabilidad de las empresas de respetar los derechos humanos, se señala que ello aplica “a todas las empresas, independiente del lugar de sus operaciones, tamaño, sector, contexto operacional, propietario y estructura, y en toda su cadena de valor”. Tal respeto exige de las empresas, de acuerdo a lo señalado en el plan, entre otros, “[q]ue apliquen la debida diligencia en materia de derechos humanos con el fin de identificar los potenciales riesgos de impactos en derechos humanos en el contexto de sus operaciones”; y, “[q]ue establezcan mecanismos operacionales de reclamación que les permitan identificar potenciales impactos y repararlos en caso de que sucedan”.

5. Describir avances y desafíos en la implementación de marcos normativos y políticas públicas anteriormente mencionados. En lo posible, indicar las razones que explican estos desafíos y los esfuerzos desarrollados para superarlos.

Respecto a los desafíos de la **protección de datos personales** por parte de las empresas, podemos nombrar:

- Eficiencia para las y los usuarios

Como reconoce Alberto Cerda (2011),[48] el constitucionalismo latinoamericano ha sido, comparativamente, más eficiente en la protección del derecho a los datos personales que las protecciones constitucionales desarrolladas en otros países, pero aquello no significa que sea una solución eficiente pues cuenta con altos costos transaccionales, la ineficiencia en la prevención del incumplimiento, la falta de stare decisis de las decisiones judiciales -ya que, salvo contadas excepciones, sólo aplican al caso sujeto a decisión judicial, y la generalidad de las previsiones constitucionales (dejando así mucho margen para la interpretación judicial). Asimismo, Milanes (2017) de ADC Argentina, en su revisión de sistemas de protección de datos de Argentina, México, Chile y Brasil, concluye que “a pesar de contar con un soporte constitucional que aparece como robusto, en la práctica generan un escenario que se caracteriza por su disparidad y fragmentación, con debilidades estructurales y una relativa –más bien negativa– capacidad de enforcement”.

- Modernización

Muchas de las leyes de protección de datos personales en nuestro continente necesitan de una importante y urgente modernización, que responda a los vertiginosos avances tecnológicos que generan desafíos que trascienden límites geográficos. Milanes (2017) , por ejemplo, distingue desafíos como: los principios de minimización y responsabilidad proactiva, o el derecho a la portabilidad y el

[48] Hacia una Internet libre de censura. Propuestas para América Latina http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf

mayor detalle y análisis de viabilidad de medidas concretas en cabeza de los responsables que aseguren el mejor tratamiento posible de los datos personales. Asimismo, destaca el necesario diálogo para el fortalecimiento de la autodeterminación informativa y su confluencia con otros derechos humanos: “La contundencia del derecho a la autodeterminación informativa, en tanto garantiza al individuo el control de sus datos, genera innumerables y permanentes situaciones de conflicto con otros derechos, también esenciales para su adecuado desarrollo. Más allá de las vías procedimentales y judiciales, en las que en última instancia transcurrirán y se resolverán los conflictos en cuestión, la generación de espacios de interacción y diálogo que posibiliten el debate riguroso, experto y permanente de las diversas situaciones de confluencia de los derechos en cuestión posibilitará la generación de experiencia e insumos que redunden en un fortalecimiento del ejercicio del derecho a la autodeterminación informativa como parte integrante del conjunto de derechos humanos del individuo”.

- Armonización legislativa

El incremento en el flujo transfronterizo de datos pone de manifiesto la necesidad de incluir a la armonización legislativa como un aspecto de relevancia no sólo para el fortalecimiento de los propios sistemas de protección de datos, sino también con miras en el desarrollo de la economía digital de los países en cuestión y de la región. Asimismo, la entrada en vigencia de marcos legales tan importantes como el GDPR (Reglamento General de Protección de Datos) de la Comisión Europea, seguramente supondrá un impulso para adoptar o actualizar las normativas nacionales existentes. De este modo, el desafío es lograr una acción coordinada por parte de los Estados para que todas las personas gocen de los mismos derechos, sin importar el país del sistema interamericano al que pertenezca. En este sentido, la fragmentación de los sistemas nacionales constituye un desafío serio. En nuestro continente, coexisten países con leyes generales de protección de datos con otros que carecen de ella. Asimismo, algunos países cuentan con una autoridad de protección de datos independiente mientras que otros no cuentan con ella. Así, resulta imperioso avanzar lo más pronto posible en la constitución de una agenda común para establecer estándares comunes. Para ello, la CIDH está en una inmejorable posición para impulsar el proceso.

- *Enforcement*.

Un aspecto especial de la protección de datos es la capacidad de los Estados para poder hacer cumplir las leyes. De esta manera, aunque los países cuenten con leyes eficaces y actualizadas, la falta de un órgano fuerte que pueda inspeccionar, vigilar o sancionar violaciones impide que en la práctica la ley tenga alguna eficacia. Tal como lo dijimos en el punto anterior, varios países del sistema interamericano carecen de un autoridad de protección de datos. Pero incluso entre aquellos que sí la tienen, la situación no es mucho mejor. Sea por ausencia de autonomía o independencia, o por la carencia de recursos económicos y técnicos suficientes, no existe una capacidad de *enforcement* eficaz para controlar el cumplimiento por parte de las empresas. De esta manera, otro desafío es implementar políticas públicas que tomen en serio la protección de datos a través de la creación o la jerarquización y fortalecimiento de los mecanismos estatales existentes para ese fin.

Respecto a los desafío del uso de **big data** por parte de las empresas, podemos nombrar:

- Ponderación de beneficios

Las políticas públicas que se centren en su utilización o en el incentivo de modelos de negocios por parte de los privados que se funden en el uso de tal tecnología, deben ponderar sus beneficios con la evaluación de los nuevos problemas que se enfrentan, tanto en su uso por el Estado como por las empresas privadas. Como dice Fundación Karisma de Colombia, "por esta razón, es recomendable no desmontar los desarrollos actuales en favor del derecho a la intimidad y de la protección de datos con el único propósito de permitir la ejecución de la política de big data. Por el contrario, los riesgos que hemos referido antes tienen que servir para que estas protecciones se mantengan, refuercen y actualicen".

En este sentido, como reconoce la Information Commissioner's Office (ICO) del Reino Unido en un documento particular sobre esta temática,[49] debe tenerse siempre presente que el big data, la inteligencia artificial y el machine learning (aprendizaje automático), si bien pueden verse cada vez más como "negocios normales", sus características representan un cambio radical en el procesamiento

[49] Big data, artificial intelligence, machine learning and data protection https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

de los datos personales. Estas implicaciones, según ICO, surgen no sólo por el volumen de los datos, sino de las formas en que se genera, la propensión a encontrar nuevos usos para él, la complejidad del procesamiento y las posibles consecuencias inesperadas para las personas.

Respecto a los desafíos de la **cibervigilancia** por parte de las empresas, podemos nombrar:

- Evaluación previa y permanente del cumplimiento de DDHH

El principal y más grande desafío es lograr el reconocimiento por parte de los Estados de su obligación de aplicar a cualquier iniciativa que implique la implementación de cibervigilancia un marco de evaluación previa y permanente del cumplimiento de sus obligaciones internacionales de derechos humanos.

En la actualidad, en nombre de la seguridad nacional, de la seguridad pública o de la eficiencia en la entrega de servicios estatales, se encuentran implementadas o en vía de implementación numerosas iniciativas en la región que abarcan, por ejemplo: el uso de biometría, cámaras de alta definición o reconocimiento facial en espacios públicos, dispositivos de vigilancia como drones o globos aerostáticos equipados con cámaras de alta definición, equipos de interceptación de señales telefónicas (IMSI-catcher) y softwares maliciosos de interceptación de telecomunicaciones. La mayor parte de estas iniciativas se gestan en forma administrativa, sin transparencia y debate democrático por parte de los órganos legislativos, y todas ellas tienen en común la adquisición a empresas de las tecnologías que hacen posible estas modalidades de cibervigilancia.

Urge como región un pronunciamiento claro de los órganos del Sistema Interamericano acerca de la obligación de los Estados de la región de someterse en el desarrollo de este tipo de políticas a los estándares de protección de los derechos humanos a los cuales se encuentran obligados por los instrumentos del sistema regional antes enunciados, con explícita referencia al rol que cabe a las empresas como proveedoras de tales tecnologías.

- Agenda de transparencia y anticorrupción

Las denuncias de espionaje contra activistas, opositores políticos y periodistas se acumulan, y abren el debate sobre la necesidad de transparentar la adquisición de tecnología de inteligencia y vigilancia, así como la urgencia de regular las intervenciones gubernamentales de comunicaciones. Como se expresó en el documento "Recomendaciones para la transparencia y anticorrupción en la adquisición y uso de tecnologías de vigilancia por parte de los Estados Americanos" y que se hizo en el marco de la Cumbre de las Américas realizada en abril del 2018 en Perú, "como los principales compradores en el mercado, no hay duda de que son los Estados los que deben impulsar también un mercado transparente y apegado a los derechos humanos. Los estados deben avanzar en obligar a las empresas proveedoras de tecnologías de vigilancia, tanto las de nuestro continente como las extranjeras que hacen negocios multimillonarios en nuestros países, a tener un marco de comportamiento que asegure el respeto a los derechos humanos, a la gobernabilidad democrática y a la transparencia y anticorrupción de los procesos de venta".[50]

6. Mencionar cuáles son los indicadores y mecanismos interinstitucionales oficiales para monitorear y/o evaluar estos avances y desafíos. En caso no existan, qué indicadores y mecanismos generales identifica como los más adecuados.

- Respecto a protección de datos

Estándares internacionales que resultan útiles en la orientación para enfrentar los desafíos indicados en la respuesta anterior son los propuestos por la OCDE, el Convenio 108 de la Unión Europea, los Estándares de Protección de Datos de los Estados Iberoamericanos y el recientemente dictado Reglamento General de Protección de Datos de la Unión Europea (GDPR).

[50] Recomendaciones para la transparencia y anticorrupción en la adquisición y uso de tecnologías de vigilancia por parte de los Estados americanos https://www.derechosdigitales.org/wp-content/uploads/Recomendaciones-para-la-transparencia-y-anticorrupcion-en-la-compra-y-uso-de-tecnologias-de-vigilancia-por-parte-de-los-Estados-americanos.pdf

En particular, la Red Iberoamericana de Protección de Datos (RIPD) estrenó el 2017 los "Estándares de Protección de Datos de los Estados Iberoamericanos",[51] que son directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de protección de datos en aquellos países de la región iberoamericana que no cuentan con estos ordenamientos o que sean referentes para la modernización y actualización de las legislaciones existentes.

Para la elaboración de los Estándares Iberoamericanos se tomaron como referencia algunos instrumentos internacionales como las Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y Desarrollo Económicos (OCDE); el Convenio número 108 del Consejo de Europa y su Protocolo; el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico y el Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas en lo relacionado con el tratamiento de datos personales y la libre circulación de estos datos, entre otros.

Los objetivos de esos "Estándares de Protección de Datos de los Estados Iberoamericanos" son: (i) establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región, (ii) garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales, (iii) facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región, y (iv) favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y organismos internacionales en la materia.

El estándar 5.1 estipula que los principios serán aplicables a todo responsable o encargado que haga tratamientos de datos relacionadas con la oferta de bienes o servicios dirigidos a los residentes de los Estados Iberoamericanos, o bien, estén relacionadas con el control de su comportamiento, **aunque no estén establecidos en el territorio de un Estado Iberoamericano.** Este principio resulta de particular importancia, debido a que varias de las más grandes empresas que realizan tratamiento de datos tienen su sede en otros países y suelen esgrimir este motivo para evitar sujetarse a las leyes y jurisdicción de los estados nacionales.

Por otro lado, los estándares mencionan una serie de principios que todo responsable o encargado de tratamiento de datos debe cumplir. Entre aquellos que pueden generar un alto impacto en las actividades empresarias, podemos mencionar los siguientes:

- Principio de Responsabilidad (numeral 20.1): "El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes Estándares, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines".
- Principio de Seguridad (numeridas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales".
- Principio de Confidencialidad (numeral 23.1) "El responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular."

A los fines de ayudar al cumplimiento de los principios recién mencionados -y los demás previstos en los estándares- se promueve la implementación de "Medidas proactivas en el tratamiento de datos personales".

---

[51] ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS
http://www.redipd.org/noticias_todas/2017/novedades/common/Estandares_de_proteccion_de_datos_personalesmparalos_estados_iberoamericanos.pdf#Estandares%20PD

Entre las disposiciones más destacadas, se encuentra la necesidad de designar un Oficial de Protección de Datos (numeral 39), que será el encargado de asesorar, coordinar y supervisar internamente el cumplimiento de la legislación sobre protección de datos personales por parte de la organización. La presencia de este oficial es requerida en los casos de que el tratamiento tenga por objeto "una observación habitual y sistemática de la conducta del titular" o "sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales".

Por otro lado, se establece que cuando un tratamiento de datos personales "por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación..." se deberá realizar de manera previa una evaluación de impacto.

En tanto las actividades empresariales relacionadas con tecnología, big data y cibervigilancia implica la probable utilización de técnicas de tratamiento masivos de datos personales, queremos resaltar estos estándares ya que pueden servir como herramienta para contener potenciales abusos por parte de las compañías.

- Respecto a big data

La recientemente lanzada “Declaración de Toronto: Protegiendo los derechos a la igualdad y la no discriminación de los sistemas automatizados”,[52] preparada por un grupo de organizaciones de derechos humanos que trabajan a nivel internacional, se propone un marco de principios emanados de la aplicación del marco internacional de protección de derechos humanos que resulta útil para guiar la acción de empresas y Estados en esta materia, que abarca pero va mucho más allá del big data, para alcanzar las decisiones algorítmicas y la inteligencia artificial.

La declaración propone que “los Estados y los actores privados deberían promover el desarrollo y el uso de estas tecnologías para ayudar a las personas a ejercer y disfrutar más fácilmente de sus derechos humanos. Por ejemplo, en el cuidado de la salud, los sistemas de aprendizaje automático podrían aportar avances en diagnósticos y tratamientos, al tiempo que podrían hacer que los servicios de salud estén más ampliamente disponibles y sean más accesibles. Los Estados y los actores privados deberían promover, en términos más generales, el derecho positivo al disfrute de los beneficios del progreso científico y sus aplicaciones en relación con el aprendizaje automático y la inteligencia artificial, como una afirmación de los derechos económicos, sociales y culturales. Pero agrega: “Los derechos a la igualdad y la no discriminación son solo dos de los derechos humanos que pueden verse afectados por el uso de sistemas automatizados: privacidad, protección de datos, libertad de expresión, participación en la vida cultural, igualdad ante la ley y acceso significativo a remedios son solo algunos de los otros derechos que pueden dañarse con el uso indebido de esta tecnología. Los sistemas que toman decisiones y procesan datos también pueden implicar derechos económicos, sociales y culturales; por ejemplo, pueden tener un impacto en la provisión de servicios y oportunidades tales como la atención médica y la educación, y el acceso a oportunidades, como la mano de obra y empleo”. La declaración cierra con la declaración de las obligaciones y las empresas en estas materias, proveyendo un marco de análisis para las mismas.

- Respecto a derechos humanos en la industria de la cibervigilancia

En este sentido, parece interesante avanzar desde la base de los “Principios globales sobre seguridad nacional y el derecho a la información”, también conocidos como “Principios de Tshwane”.[53] Estos han sido formulados para orientar a quienes intervienen en la redacción, revisión o implementación de leyes o disposiciones relativas a la potestad del Estado para clasificar información por motivos de seguridad nacional o sancionar su divulgación. Estos principios definen que las “Compañías dentro del sector de la seguridad” es una "persona jurídica que lleva a cabo o ha llevado a cabo transacciones o negocios en el sector de la seguridad nacional, y solamente en tal calidad; ya sea como contratista o proveedor de servicios, instalaciones, personal o productos incluyendo, aunque sin limitarse a, armamento, equipos e inteligencia. Esto incluye empresas militares y de seguridad privadas

[52] The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems https://www.accessnow.org/cms/assets/uploads/2018/05/Toronto-Declaration-D0V2.pdf

[53] Principios globales sobre seguridad nacional y el derecho a la información (“Principios de Tshwane”) https://www.opensocietyfoundations.org/sites/default/files/tshwane-espanol-10302014%20%281%29.pdf

(PMSCs)". Se reconoce que estas compañías tienen distintos tipos de responsabilidad con la protección de los derechos humanos. En este sentido, parecen pertinentes los siguientes principios:

Principio 1: Derecho a la información
(a) Los principios internacionales también reconocen que las empresas dentro del sector de seguridad nacional, incluidas las empresas militares y de seguridad privadas, tienen la responsabilidad de divulgar información con respecto a situaciones, actividades o conductas que razonablemente se puede esperar que tengan un impacto en el ejercicio de los derechos humanos.

(c) Aquellos que tengan la obligación de divulgar información, de acuerdo con los Principios 1(a) y 1(b), deben proporcionar la información que se solicite y tienen una obligación positiva de publicar información de interés público, salvo las limitadas excepciones previstas en la legislación que sean necesarias para prevenir perjuicios concretos e identificables a intereses legítimos, incluida la seguridad nacional.

(e) Cualquier argumentación de seguridad nacional hecha por una empresa para justificar la clasificación de información ha de ser explícitamente autorizada o confirmada por una autoridad pública cuyas responsabilidades incluyan la protección de la seguridad nacional.

Asimismo, los Principio 2 y 3 de Aplicación de los Principios y de Requisitos para restringir el derecho a la información por razones de seguridad nacional deberían también ser concernientes a las empresas privadas.

Por su parte, el "Principio 10: Categorías sobre las cuales existe una fuerte presunción o un interés preponderante a favor de su divulgación", enumera causas que revisten un interés público especialmente significativo para el proceso de control democrático y el Estado de derecho, por lo que hay una necesidad imperiosa de que tal información debería ser pública y divulgarse en forma proactiva.

A su vez, y respecto a la necesidad de transparencia y acceso a la información en el sector de la seguridad, parece atingente el Principio 34 "Transparencia de los organismos de supervisión independientes", que determina que "los órganos de supervisión deben estar legalmente obligados a elaborar informes periódicos y a hacerlos públicos. Dichos informes deben incluir, como mínimo, información sobre el propio órgano supervisor, incluidas sus funciones, integración, presupuesto, desempeño y actividades", a lo que se debe agregar "información acerca de las funciones, estructura, presupuesto y actividades generales de cualquier institución del sector de la seguridad que no divulgue por sí misma dicha información al público". Asimismo, se especifica que deben proporcionar "la mayor cantidad de información posible sobre cuestiones de interés público, incluidas las áreas enumeradas en el Principio 10".

En esta misma materia, los Principios Internacionales Necesarios & Proporcionados sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones[54] acordados en 2014 por grupos de la sociedad civil, representantes de la industria y expertos internacionales en legislación sobre Vigilancia de las Comunicaciones, políticas públicas y tecnología, proporcionan una guía para clarificar cómo se aplica el derecho internacional de los derechos humanos en relación a las tecnologías y técnicas de vigilancia de las Comunicaciones, y a su vez permiten evaluar contra ellos el accionar de la industria y los Estados para determinar si las leyes y prácticas de vigilancia que desarrollan, actuales o propuestas, están en línea o no con los derechos humanos.

7. Proporcionar información sobre buenas prácticas destinadas al cumplimiento de estándares de derechos humanos en el marco de actividades empresariales.

Existen algunas iniciativas de la sociedad civil y del mundo académico que han avanzado en trabajar buenas prácticas para la recolección y tratamiento de datos, la protección de la privacidad y las decisiones automatizadas. Cabe destacar que aún falta trabajar en buenas prácticas, desde un punto de vista regional y multisectorial, adecuadas en los contextos tecnológicos actuales, no obstante, las iniciativas descritas a continuación son un buen pie inicial para el avance en este sentido.

---

[54] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones https://necessaryandproportionate.org/es/necesarios-proporcionados

La Asociación por los Derechos Civiles de Argentina, entre el 2015 y el 2016, realizó un estudio de las prácticas y políticas empresariales para analizar el efectivo cumplimiento de la legislación en vigencia sobre protección de datos personales en países como Argentina, Brasil, Chile y México. Con base en dicha investigación, se proponen las siguientes recomendaciones.

Transparencia: Las empresas deben publicar periódicamente reportes de transparencia acerca de la forma en que realizan el tratamiento de los datos de las personas incluidas en sus bases. Este informe debe incluir: identificación de las autoridades que soliciten datos personales, número de usuarios y usuarias afectados, información sobre el cumplimiento o rechazo de las solicitudes y los motivos por los cuales se tomó una decisión u otra, estadísticas sobre los tipos de datos solicitados y justificación legal de la solicitud, entre otros.

Información clara y accesible: Las personas deben poder saber con detalle la forma en que las empresas van a realizar el tratamiento de sus datos. Por lo tanto, éstas deberían difundir sus políticas de privacidad en un lugar de fácil acceso. En este sentido, su colocación al pie de página de los sitios web mediante una leyenda que las identifique claramente resulta un paso necesario pero no suficiente, ya que deben ser complementadas con información que amplíe y especifique las operaciones que la empresa lleva a cabo con los datos de las personas. Por lo tanto, no se ajusta al deber de información que las políticas difundidas solo se limiten a repetir lo que dicen las leyes vigentes.

Notificación a las y los usuarios: Las empresas deberían notificar a las y los usuarios de manera inmediata las situaciones que puedan afectar o ya afectaron de manera intensa la protección de sus datos personales. Dentro de estas situaciones, la necesidad de informar acerca de solicitudes de información de datos por parte de las autoridades y sobre la existencia de prácticas de retención de datos y/o vigilancia encubierta se vuelve imprescindible debido a los riesgos que estas conductas plantean al ejercicio de determinados derecho y garantías, como la intimidad o el debido proceso. En este sentido, las empresas no deberían entregar datos sin mediar una orden judicial o expresa obligación legal.

Términos y condiciones que respeten la dignidad de las personas: El manejo que las empresas realizan de los datos personales de sus usuarios suele estar contemplado en los «términos y condiciones» que cada persona debe aceptar antes de poder contratar un servicio. Al estar compuestos de largas y engorrosas páginas con letra chica y lenguaje técnico, se vuelve muy dificultoso acceder a la política de privacidad contenida en ellos. Por lo tanto, las empresas deberían implementar documentos que de manera sencilla y mediante un lenguaje accesible, cumplan con el deber de informar de manera clara y detallada a los usuarios acerca de las políticas que llevarán a cabo con sus datos y evitar modificaciones unilaterales sin conocimiento de los usuarios.

Mayor apertura a la sociedad civil: Al ser actores privados, las empresas suelen estar fuera del alcance de ciertas obligaciones que le atañen al sector público, como el deber de brindar información, reconocido por las leyes de acceso a la información pública. Por lo tanto y como parte de un proceso de transparencia, las empresas deberían ser más receptivas a los pedidos de organizaciones de la sociedad civil que buscan conocer sus prácticas de tratamiento de datos. Esto implicaría la respuesta positiva a los pedidos de información, la disposición de participar en entrevistas o mesas de trabajo y cualquier otro comportamiento que implique la voluntad de empresas a involucrarse en un diálogo inclusivo con todos los sectores interesados en la protección de los datos personales.

En la línea de estas recomendaciones, también existe la iniciativa llamada "Quién Defiende tus Datos",[55] la cual es liderada por la ONG de Estados Unidos, Electronic Frontier Foundation (EFF), y que de forma más específica establece seis criterios para evaluar las prácticas y políticas de privacidad de las empresas de telecomunicaciones: *Políticas de privacidad y protección de datos personales, Autorización judicial, Notificación al usuario, Posicionamiento público en contra de la vigilancia masiva o sin control, Transparencia, y Bloqueo de contenidos en internet.* ONGs locales de diversos países del continente, como Argentina, México, Chile o Paraguay han aplicado estos criterios de evaluación a las telecomunicadoras que operan localmente, a manera de rankear su protección a los datos de las y los usuarios.

Asimismo, también existe la iniciativa internacional “Digital Ranking Rights” que, valorando diversas empresas del sector de la tecnología de la información y las comunicaciones, elabora un ranking de

[55] ¿Quién Defiende Tus Datos? https://qdtd.tedic.org/

acuerdo a estándares globales sobre cómo éstas deben respetar la libertad de expresión y privacidad. Así, por ejemplo, algunas recomendaciones generales desde su Index 2018, son:[56] Las empresas deben divulgar y explicar cómo cumplen con las leyes y qué significa ese cumplimiento para las y los usuarios; llevar a cabo evaluaciones periódicas para determinar el impacto de los productos, servicios y operaciones comerciales de la compañía en la libertad de expresión y privacidad de las y los usuarios; publicar informes de transparencia que incluyan el volumen, la naturaleza y la base legal de las solicitudes hechas por los gobiernos y otros terceros para acceder a la información de las y los usuarios; llevar a cabo evaluaciones periódicas para determinar el impacto de los productos, servicios y operaciones comerciales de la compañía en la libertad de expresión y privacidad de las y los usuarios. Asimismo, se plantea que los mecanismos de reclamo y los procesos de reparación por parte de las empresas deben estar disponibles de manera más prominente para las y los usuarios, entre otras tantas recomendaciones de buenas prácticas.

Respecto a big data, machine learning e inteligencia artificial, vale la pena mirar las recomendaciones de buenas prácticas que hace ICO en el Reino Unido a todo organismo que utilice estas técnicas, entre las que se encuentran: Considerar técnicas apropiadas para anonimizar los datos personales en su (s) conjunto (s) de datos (en el caso que se haga procesamiento de datos); ser transparente acerca de su procesamiento de datos personales mediante el uso de una combinación de enfoques innovadores con el fin de proporcionar avisos de privacidad significativos en las etapas apropiadas a lo largo de un proyecto de big data; incorporar un marco de evaluación de impacto de la privacidad en sus actividades de procesamiento de big data para ayudar a identificar los riesgos de privacidad y evaluar la necesidad y la proporcionalidad de un proyecto determinado; adoptar un enfoque de privacidad por diseño en el desarrollo y la aplicación de su análisis de Big Data; implementar técnicas innovadoras para desarrollar algoritmos auditables de aprendizaje automático; y desarrollar principios éticos para ayudar a reforzar los principios clave de protección de datos.

En este último aspecto, por ejemplo, la Association for Computing Machinery (ACM) avanzó en un set de principios para la transparencia y rendición de cuentas de los algoritmos.[57] Además, recientemente, una coalición de grupos relacionados a la tecnología y los derechos humanos lanzó la "Declaración de Toronto", la cual se concentra en la obligación de evitar que los sistemas de aprendizaje automático discriminen y, en algunos casos, violen las leyes de derechos humanos existentes.[58]

8. Emitir observaciones y comentarios sobre las obligaciones y estándares jurídicos internacionales, en particular aquellos provenientes del Sistema Interamericano de Derechos Humanos, que considera aplicables a los Estados miembros de la OEA respecto al establecimiento e implementación de marcos regulatorios en materia de empresas y derechos humanos, incluyendo aplicación extraterritorial en caso proceda.

La obligación de establecer marcos regulatorios en esta materia surge primariamente del artículo 1.1 de la Convención Americana sobre Derechos Humanos que establece las obligaciones de respeto y garantía y la obligación de no discriminación. La obligación de respeto impone la obligación de “no violar” directa o indirectamente los derechos humanos de las personas. La obligación de garantía supone la obligación del Estado de ordenar todo su aparato gubernamental a fin de generar las condiciones para el pleno goce y ejercicio de los derechos humanos. Además, la obligación de garantía supone la adopción por parte del Estado de medidas razonables de prevención de violaciones a los derechos humanos, incluso entre particulares; y la adopción de medidas de investigación, sanción y reparación cuando las violaciones ocurrieran.

Además, el artículo 2 de la CADH establece la obligación de adecuar la legislación interna a las obligaciones establecidas en la CADH, suponiendo la adopción de normas tendientes a garantizar dichos derechos y la derogación de normas violatorias de los mismos.

En conjunto, los artículos 1 y 2 de la CADH, proveen el marco de obligaciones generales del Estado en materia de derechos humanos y resultan aplicables a la regulación de la actividad empresarial,

---

[56] Recommendations https://rankingdigitalrights.org/index2017/findings/recommendations/
[57] Statement on Algorithmic Transparency and Accountability https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf
[58] The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/

máxime cuando dicha actividad impacta directamente en el goce y ejercicio de derechos humanos, como en este caso. Se han detallado a lo largo de este texto, algunas de las problemáticas vinculadas a las prácticas de las empresas y su impacto en los derechos humanos, en este caso, de las y los usuarios de tecnología. Dichas problemáticas conciernen a los derechos a la igualdad y no discriminación, privacidad, a la libertad de expresión, el acceso a la informacion, los derechos de asociacion y reunion, y derechos económicos, sociales y culturales. En lo que concierne a los Estados, el SIA cuenta con precedentes importantes en torno a las obligaciones de respeto y garantía asociadas a cada uno de los derechos individualmente reconocidos en la CADH.

En el marco universal, el Pacto Internacional de Derechos Civiles y Políticos establece obligaciones similares en sus artículos 2 y 3. Y específicamente Los Principios de Naciones Unidas sobre Empresas y Derechos Humanos,[59] construyen sobre las obligaciones del Estado en materia de respeto y garantía. Este último instrumento, en su primera parte establece la obligación de los Estados de adoptar normas tendientes a proteger y garantizar los derechos humanos y a prevenir la violación de los mismos por parte de terceros, incluidas las empresas; y establece además la obligación de regular la actividad empresaria para prevenir, y en su caso reparar, posibles violaciones a los derechos humanos generadas por o a instancias de estos actores.

c) Bloque 3: Prevención y supervisión

9. Identificar y describir mecanismos locales, regionales o internacionales existentes para abordar acciones de prevención, debida diligencia y supervisión relacionadas con el ejercicio de derechos humanos en el contexto de actividades empresariales. Especifique pertinencia y obstáculos del mecanismo.

La respuesta a esta pregunta se puede inferir de la respuesta a la pregunta 6 de este cuestionario.

10. Proporcionar información en materia de prevención, debida diligencia y supervisión en los Estados de origen de empresas involucradas en violaciones de derechos humanos en territorios de terceros Estados. Especifique pertinencia y obstáculos del mecanismo.

11. Emitir observaciones y comentarios sobre las obligaciones y estándares jurídicos internacionales, en particular aquellos provenientes del Sistema Interamericano de Derechos Humanos, que considera aplicables a los Estados miembros de la OEA en materia de prevención, debida diligencia y supervisión en materia de empresas y derechos humanos, incluyendo aplicación extraterritorial en caso proceda.

d) Bloque 4: Investigación, Rendición de Cuentas y Reparación

12. Identificar y describir mecanismos judiciales y no judiciales existentes a nivel local, regional e internacional que abordan violaciones de derechos humanos vinculadas a actividades empresariales, ¿cuáles son y qué efectividad tienen los recursos disponibles para las personas y comunidades afectadas? En ese marco, proporcionar información sobre decisiones judiciales y/o no judiciales relevantes sobre la materia que se hayan emitido o estén en proceso de emitirse. Identificar y describir importancia de la decisión y, en lo posible, adjuntar las decisiones o pronunciamientos respectivos.

Específicamente en materia de vigilancia, resulta pertinente hacer referencia al caso de México, en donde el Poder Judicial Federal ha reconocido el interés legítimo para combatir normas que contemplan facultades encubiertas de intromisión en el derecho a la privacidad, intimidad y protección de datos personales. Por ejemplo, en el Juicio de Amparo 116/2014, el Juzgado Segundo de Distrito en Materia Administrativa, Especializado en Competencia Económica, Radiodifusión y Telecomunicaciones, consideró que diversos artículos de la Ley Federal de Telecomunicaciones y Radiodifusión que contemplan medidas de acceso y tratamiento de datos personales pueden ser combatidas como normas autoaplicativas, reconociendo que dada la secrecía con la que se origina tanto la solicitud como el desahogo de los requerimientos de información y localización geográfica en

[59] El Consejo de Derechos Humanos hizo suyos los Principios Rectores en su resolución 17/4, de 16 de junio de 2011. http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf

tiempo real, es prácticamente imposible para la persona afectada tener conocimiento de la existencia de dicha afectación. Por tanto, la decisión estipula que, tratándose de esta clase de requerimientos de carácter confidencial, reconociendo que los mismos implican la probable afectación de derechos fundamentales como el derecho a la vida privada, la persona afectada puede controvertir su constitucionalidad sin requerir demostrar previamente un acto de aplicación, en función de que la afectación a su esfera de derechos se materializa con la mera entrada en vigor de los preceptos normativos que prevean tales requerimientos.

Asimismo, la decisión admite que requerirle a la persona que se ha visto vulnerada por este tipo de medidas el demostrar un acto de aplicación o afectación previa derivado de éstas, restringiría su derecho fundamental de acceso a un recurso judicial efectivo, ya que condicionar su impugnación de la medida respectiva, hasta en tanto tuviera conocimiento del resultado obtenido con la realización de la misma, indudablemente reduciría o, incluso, anularía la posibilidad de que se le restituya el pleno goce de sus derechos indebidamente afectados, ante una eventual sentencia protectora.

Además, respecto de los mismos preceptos normativos de la Ley Federal de Telecomunicaciones y Radiodifusión, para efectos de alcanzar un óptimo grado de certidumbre jurídica así como de enmarcar adecuadamente la actuación de las autoridades en esta materia, la Segunda Sala de la Suprema Corte de Justicia de la Nación, especificó de manera exhaustiva, mediante el amparo en revisión 964/2015, aquellas instancias de seguridad, procuración y administración de justicia que pueden ejercer las facultades previstas en dichos preceptos.[60]

13. Describir obstáculos (jurídicos y prácticos) para la reparación integral y el acceso a la justicia de víctimas de violaciones a derechos humanos relacionadas con actividades empresariales en el hemisferio americano.

Un obstáculo para la reparación integral y el acceso a la justicia de víctimas de vigilancia identificado en la región corresponde al caso de México, referido anteriormente. En este caso, la agencia encargada de llevar a cabo la investigación, la Procuraduría General de la República (PGR), es a su vez la única institución de gobierno que ha reconocido oficialmente haber adquirido el malware Pegasus con el que se intentó espiar a los y las periodistas, personas de derechos humanos y activistas en el país, mismo que como ya se señaló, se comercializa exclusivamente a gobiernos por parte de la empresa israelí NSO Group. Consecuentemente, a casi un año de que las víctimas presentarán la denuncia correspondiente, no se ha presentado ningún avance significativo en la investigación.

Por ejemplo, en el expediente, la Agencia de Investigación Criminal (AIC) órgano adscrito a la PGR, ha aceptado que adquirió las licencias de uso de Pegasus y que el equipo desde el cual se opera dicho

---

[60] **LOCALIZACIÓN GEOGRÁFICA EN TIEMPO REAL DE LOS EQUIPOS DE COMUNICACIÓN MÓVIL PREVISTA EN EL ARTÍCULO 190, FRACCIÓN I, DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN. AUTORIDADES COMPETENTES PARA SOLICITARLA Y PRESUPUESTOS QUE LA AUTORIZAN.**
Si bien la mencionada disposición legal hace referencia expresa a las "instancias de seguridad, procuración y administración de justicia" como las autoridades con que los concesionarios de telecomunicaciones y los autorizados deben colaborar en la localización geográfica en tiempo real de los equipos de comunicación móvil, lo cierto es que a fin de lograr un óptimo grado de certidumbre jurídica a los gobernados, así como enmarcar adecuadamente la actuación de las autoridades en esta materia, se considera que las autoridades a que se refiere la porción normativa aludida son: (I) el Procurador General de la República, así como **los Procuradores de las entidades federativas y, en su caso, los servidores públicos en quienes deleguen esta facultad, en términos del artículo 21 de la Constitución Federal;** (II) la Policía Federal, conforme a lo previsto en el artículo 8, fracción XXVIII, de la ley que la regula; y, (III) la autoridad encargada de aplicar y coordinar directamente la instrumentación de la Ley de Seguridad Nacional en los supuestos establecidos en su artículo 5. Así, sólo las autoridades referidas podrán solicitar la localización geográfica en tiempo real de los equipos de comunicación móvil cuando se presuma que existe un peligro para la vida o la integridad de las personas, lo que implica que dicha facultad no se circunscribe a un catálogo de delitos determinado, sino que encuentra su razón jurídica en la tutela de los derechos humanos a la vida y a la integridad personal, como valor supremo a cargo del Estado mexicano.

Amparo en revisión 964/2015. Carlos Alberto Brito Ocampo y otros. 4 de mayo de 2016. Cinco votos de los Ministros Eduardo Medina Mora I., Javier Laynez Potisek, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Alberto Pérez Dayán; se apartaron de consideraciones Margarita Beatriz Luna Ramos y José Fernando Franco González Salas, este último respecto a las consideraciones relacionadas con los datos estructurados (megadatos). Ponente: Alberto Pérez Dayán. Secretario: Isidro Emmanuel Muñoz Acevedo. Décima Época, Registro: 2012191, Instancia: Segunda Sala, Tipo de Tesis: Aislada, Fuente: Gaceta del Semanario Judicial de la Federación, Libro 33, Agosto de 2016, Tomo II, Materia(s): Administrativa, Tesis: 2a. XLIV/2016 (10a.) Página: 1305

software se encuentra ubicado en sus oficinas de la Ciudad de México. No obstante, la Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión (FEADLE), a cargo del caso, no ha realizado ningún acto de investigación respecto de la AIC y la operación de NSO Group en el país, incluso cuando esto ha sido objeto de reiteradas solicitudes por parte de los denunciantes así como de recomendaciones de peritos expertos en la investigación, como Citizen Lab. La procuraduría tampoco ha identificado ni entrevistado a los agentes involucrados en la contratación de Pegasus ni en la operación del mismo, tampoco se han hecho visitas a las instalaciones en las que es operado el software ni se han revisado las cámaras de vigilancia, registros, bitácoras o medidas de seguridad implementadas en torno al uso del sistema.

Incluso, la PGR se ha negado a requerir el contrato y anexo técnico por virtud del cual se adquirió Pegasus (a pesar de que este ya se ha hecho público por la prensa). Por tanto, es fundamental señalar que desde que se evidenció el uso de este malware en México no se ha aperturado investigación alguna respecto de la trama de corrupción que podría estar detrás del uso ilegal de esta herramienta ni de las empresas intermediarias que podrían estar involucradas en la misma. Notoriamente en este sentido, han avanzado más ágilmente investigaciones periodísticas de diversos medios que la de la propia PGR.

De lo anterior se advierte que existe una evidente falta de capacidad y de voluntad política para llevar a cabo una investigación de estos hechos de manera seria, imparcial y exhaustiva; lo cual, indudablemente, constituye una vulneración y un obstáculo para la reparación integral y el acceso a la justicia de víctimas. En este sentido, tanto las víctimas como las organizaciones que las representan, entre otras, al igual que diversos organismos internacionales de derechos humanos y Relatores Especiales en materia de privacidad, libertad de expresión y protección de personas defensoras de derechos humanos, entre otros, han urgido al gobierno mexicano a implementar las salvaguardas de objetividad e imparcialidad necesarias para la investigación e incluso, a que se establezca un mecanismo extraordinario para asegurar garantías de independencia respecto de la misma, tales como la intervención de un panel de expertos y expertas independientes, que incluya la participación de mecanismos internacionales de derechos humanos.

14. Proporcionar información sobre mecanismos de investigación, rendición de cuentas y reparación integral a víctimas en los Estados de origen de empresas involucradas en violaciones de derechos humanos en territorios de terceros Estados. Especifique y adjunte información pertinente.

15. Emitir observaciones y comentarios sobre las obligaciones y estándares jurídicos internacionales, en particular aquellos provenientes del Sistema Interamericano de Derechos Humanos, que considere aplicables a los Estados miembros de la OEA sobre investigación, rendición de cuentas y reparación en materia de empresas y derechos humanos, incluyendo aplicación extraterritorial en caso proceda.

::::

Coordinadora general: Paz Peña, paz@pazpena.com

FIRMAS DE LAS ORGANIZACIONES A ESTE DOCUMENTO:

- Asociación por los Derechos Civiles, ADC, Argentina
- Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Argentina
- Coding Rights, Brasil
- Derechos Digitales, Chile y América Latina
- Fundación Karisma, Colombia
- Red en Defensa de los Derechos Digitales, R3D, México