Privatización de la seguridad y derechos humanos. Impacto de la seguridad privada y su uso de tecnologías de vigilancia

(Septiembre, 2019).

I. Introducción

Al Sur es un consorcio de organizaciones que trabajan en la sociedad civil y en el ámbito académico en América Latina y que buscan con su trabajo conjunto fortalecer los derechos humanos en el entorno digital de la región.

En ocasión del informe "Privatización de la seguridad: Impacto de la seguridad privada en los derechos humanos"[1] convocado por la Comisión Interamericana de Derechos Humanos (CIDH), en conjunto con su Relatoría Especial sobre los Derechos Económicos, Sociales, Culturales y Ambientales (REDESCA), hemos realizado un documento conjunto exploratorio de la situación de los derechos humanos cuando, en el contexto de la privatización de la seguridad en nuestro continente, se utilizan tecnologías de vigilancia.

Si bien el término de seguridad privada podría ser muy amplio, en esta oportunidad el informe se concentra en el uso de tecnologías de vigilancia por parte de la seguridad privada en el ámbito de la denominada "seguridad ciudadana". En un contexto de creciente digitalización de nuestras sociedades, esperamos que este documento pueda arrojar pistas sobre los desafíos de política pública más urgentes e importantes al respecto en el contexto de la protección de nuestros derechos humanos.

II. Usos de tecnología de vigilancia en la seguridad privada y los derechos humanos en juego

Tal como observa las Naciones Unidas en su resolución "El derecho a la privacidad en la era digital", el rápido ritmo del desarrollo tecnológico "incrementa la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, a través de la interceptación o interferencia de las comunicaciones y recopilación de datos, ya sea en las interacciones en los espacios digitales o a través del monitoreo físico de las personas en espacios privados y públicos, lo que podría constituir una violación o una transgresión de los derechos humanos, en particular del derecho a la privacidad y la libertad de expresión y de reunión, establecidos en los artículos 12, 19 y 20 de la Declaración Universal de Derechos Humanos, de los artículos 17, 19 y 21 del Pacto Internacional de Derechos Civiles y Políticos, y de los artículos 11, 13 y 15 de la Convención Americana de Derechos Humanos, respectivamente. Sin embargo, las consecuencias del monitoreo constante a través de tecnologías de vigilancia no se

[1] Cuestionario de consulta para la elaboración del Informe "Privatización de la seguridad: Impacto de la seguridad privada en los derechos humanos". OAS. 5 de septiembre 2019. https://www.oas.org/es/cidh/prensa/comunicados/2019/218.asp

reducen al mero impacto de los derechos civiles y políticos, para avanzar crecientemente en la posibilidad de que ellas impacten en la discriminación de los individuos en el acceso y ejercicio de sus derechos económicos, sociales y culturales.

Tanto el Alto Comisionado de Naciones Unidas para los Derechos Humanos como la CIDH han señalado que la interceptación de comunicaciones digitales o la recopilación de datos personales pueden afectar tanto a la libertad de expresión, de reunión y asociación pacífica, como al derecho a la vida familiar. De acuerdo a Derechos Digitales, "es por ello que mecanismos como la televigilancia, interceptación de comunicaciones, retención de data y metadatos y/o la vigilancia mediante tecnología biométrica han sido catalogados como amenazas tanto al catálogo de derechos humanos como al sistema democrático de derecho".[2]

Los usos de tecnologías de vigilancia en el marco de la privatización de la seguridad ciudadana se dan mayormente atadas a tres grandes tendencias en el continente: la tercerización a privados de labores de seguridad ciudadana por parte de los Estados, la contratación de empresas de seguridad que ofrecen estos servicios de vigilancia por parte de privados que quieren incrementar su sensación de seguridad y, muy relacionada con esta última, la integración de capacidades de vigilancia privada a sistemas estatales.

Por lejos, uno de los tipos de tecnologías de vigilancia desplegadas por privados con fines de seguridad más comunes es la televigilancia (o videovigilancia), es decir, el uso de cámaras (móviles o fijas) para fines de vigilancia. Como Ramírez y Valenzuela (2017) reconocen:[3]

> En Latinoamérica se implementan crecientemente las cámaras para combatir la delincuencia callejera y se fomenta su uso por particulares para proveerse de la seguridad pública que el estado no está otorgando. Lo anterior es promovido desde diversas organizaciones públicas y privadas, mientras que la demanda por seguridad ciudadana igualmente impulsa la aplicación de medidas de notoria visibilidad como la videovigilancia.

Con el avance de las capacidades tecnológicas, preocupa en particular el equipamiento de la televigilancia con capacidades biométricas como el reconocimiento facial. De acuerdo con un estudio regional de la Asociación por los Derechos Civiles (ADC) sobre biometría, "la narrativa que prima posiciona a la seguridad pública y a la biometría

[2] La construcción de estándares legales para la vigilancia en América Latina. Parte I: Algunos ejemplos de regulación actual en América Latina. Becker, Lara & Canales. 2018. https://www.derechosdigitales.org/wp-content/uploads/construccion-estandares-legales-vigilancia-I.pdf

[3] Videovigilancia en el espacio público: el monitoreo de la ciudad como dispositivo del control poblacional. Ramírez & Valenzuela. 2017 http://repositorio.uchile.cl/bitstream/handle/2250/146569/Videovigilancia-en-el-espacio-p%C3%BAblico-el-monitoreo-de-la-ciudad-como-dispositivo-del-control-poblacional.pdf?sequence=1&isAllowed=y

como la pareja definitiva para solucionar los mayores problemas de inseguridad, siendo utilizada para la investigación y la lucha contra el delito".[4]

Esta tecnología facilita la captura, almacenamiento y procesamiento de la información biométrica de las personas, es decir, sus rasgos biológicos, morfológicos y de comportamiento, que luego son convertidos en una matriz o plantilla comparable que puede ser leída por computadoras. Una vez que estas plantillas digitales son vinculadas con el perfil de una persona, pueden usarse para verificar la identidad en un proceso de probabilidades y no de certezas. Como reconoce ADC: "En el caso del reconocimiento facial, los algoritmos encargados de encontrar las similitudes entre las plantillas con los rasgos faciales pueden contener sesgos derivados de su programación y/o entrenamiento".

Particularmente, respecto a estas tecnologías biométricas y de acuerdo con un informe de TEDIC, "tanto el ex Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión (ONU), Frank La Rue y el Alto Comisionado de Derechos Humanos (ONU), Navi Pillay, han expresado preocupación por las violaciones del derecho a la intimidad debidas a la falta de medidas de protección eficaces en la utilización de tecnologías biométricas".[5]

Y aunque no son tan comunes, también crecientemente se integran a la privatización de la seguridad el uso de aplicaciones de rastreo y geolocalización -desarrolladas por empresas privadas- y que buscan denunciar actividades sospechosas, potencialmente delincuenciales. La recolección de datos, su uso y su manejo abusivo por parte de estas apps pueden poner en entredicho derechos humanos como la privacidad de sus usuarios y generar riesgos adicionales de discriminación y marginalización de sectores de la población vulnerables o tradicionalmente discriminados.[6]

Existen diversos ejemplos en el continente que han alertado tanto a organizaciones de la sociedad civil como a la misma opinión pública en cuanto a los efectos de estos usos de tecnologías de vigilancia por parte de privados en los derechos humanos de las personas y en su acceso y ejercicio de derechos económicos, sociales y culturales:

a) Tercerización a privados de labores de seguridad ciudadana por parte de los Estados:

En **Chile**, por ejemplo, a inicios del 2019, el gobierno anunció el plan Sistema de Vigilancia Móvil, que contará con una flota de 120 drones (aeronaves no tripuladas) que tendrán cámaras con capacidad de reconocimiento facial y que "combatirán la

[4] "Tu yo digital", Asociación por los Derechos Civiles (ADC), Fundación Karisma, InternetLab, Red en Defensa de los Derechos Digitales (R3D), abril de 2019, disponible en: https://adc.org.ar/wp-content/uploads/2019/06/050-tu-yo-digital-04-2019.pdf

[5] La enajenación continua de nuestros derechos. Sistemas de identidad: biometría y cámaras de vigilancia no reguladas en Paraguay. Fulchi, Carrillo & Sequera. 2018 https://www.tedic.org/wp-content/uploads/2018/07/La-enajenaci%C3%B3n-continua-de-nuestros-derechos_TEDIC_2018.pdf

[6] Christiansen, Axel. SOSAFE: La aplicación que muestra cómo Chile se cae a pedazos. La Tercera, 17 de octubre de 2017. http://mouse.latercera.com/sosafe-peores-denuncias/

delincuencia" en varias ciudades del país para el año 2020. Asimismo, se reconoció que, aunque por ahora los drones son piloteados por fuerzas policiales, "quedarán posteriormente a cargo de una empresa que tendrá que pasar por un proceso de licitación".[7] Este anuncio llevó a que diversas organizaciones de la sociedad civil se pronunciaran a través de una declaración que califica al sistema de ser contrario a los derechos humanos:[8]

> Además de ser contrario a la ley y a la Constitución, el sistema desconoce las obligaciones adquiridas por el Estado chileno en el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos. Ignora las recomendaciones de los Relatores Especiales para la Libertad de Expresión y para la Privacidad de la Organización de las Naciones Unidas, como también las de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos y las del Grupo de Trabajo de Protección de Datos de la Unión Europea (G29, Dictamen 3/2012). Incumple con principios de alto nivel y omite la opinión especializada sobre la materia.

Esta polémica se produjo solo días después que se descubriera que un operador de las cámaras de seguridad de la ciudad de Quintero, también en **Chile**, filtró imágenes de la vida privada de una mujer a su esposo.[9] La alcaldía anunció que el funcionario no es municipal, sino empleado de una tercera empresa que maneja las cámaras. El presidente del Consejo Para La Transparencia (CPLT) dijo en la oportunidad: "Son los municipios los responsables legales del tratamiento de datos personales, aunque sea un tercero el que haga los registros o trate la información", y agregó que "acá vemos cómo se vulneró el derecho a la protección de datos personales, reconocido por la Constitución y la ley, de una persona que no cometió delito alguno".[10]

Respecto a las aplicaciones de seguridad ciudadana desarrollada por privados pero de uso por diversos agentes públicos, el 2019 se supo que la app SOSAFE (con operaciones en **Chile** y **Perú**)[11] está controlada mayoritariamente por Instagis, una empresa de perfilación de votantes a través de datos personales para fines electorales, lo que dejó entrever la posibilidad de que la información de los usuarios de SOSAFE alimente las bases de datos de Instagis que se ocupan en campañas políticas o se venden a grandes

---

[7] Los "drones policía" con reconocimiento facial que vigilarán Santiago las 24 horas del día. La Tercera. 18 de marzo 2019. https://www.latercera.com/nacional/noticia/los-drones-policia-reconocimiento-facial-vigilaran-santiago-las-24-horas-del-dia/576158/

[8] Contra la vigilancia masiva en los espacios públicos del «Sistema de televigilancia móvil». Derechos Digitales. 2 de abril 2019 https://www.derechosdigitales.org/12919/contra-la-vigilancia-masiva-en-los-espacios-publicos-del-sistema-de-televigilancia-movil/

[9] Quintero: Operador de cámara de vigilancia que filtró imágenes de infidelidad de mujer fue apartado de sus funciones. Chilevisión Noticias. 31 de marzo 2019. https://www.chvnoticias.cl/sucesos/operador-camara-quintero-imagenes-infidelidad_20190331/

[10] Consejo Para la Transparencia investigará a Municipalidad de Quintero por filtración de imágenes privadas. Cooperativa. 2 de abril 2019. https://www.cooperativa.cl/noticias/pais/region-de-valparaiso/consejo-para-la-transparencia-investigara-a-municipalidad-de-quintero/2019-04-02/165203.html

[11] App de seguridad SOSAFE llega a Perú y busca crecer en América Latina. El Mercurio. 15 de octubre 2018. http://www.economiaynegocios.cl/noticias/noticias.asp?id=513166

empresas.[12] De hecho, el socio director de la aplicación, Ignacio Canals, reconoció que parte de los datos se comparten con los departamentos de seguridad municipal de cada comuna, pero negó un posible conflicto de interés. Desde Derechos Digitales, el analista Pablo Viollier señaló al mismo medio que "la utilización de información de carácter político, es decir, que dé cuenta de la inclinación política de una persona, vinculado con un individuo en particular, es ilegal sin el consentimiento del titular (…) La orientación política es un dato de carácter sensible y, por tanto, no se puede utilizar en la sección de fuentes accesibles al público, como ha pretendido Instagis".[13]

En **Paraguay**, la Policía Nacional y el Ministerio del Interior pusieron en marcha en julio de 2018 una serie de iniciativas del sistema 911 con el objeto de implementar una "tecnología biométrica" o de "reconocimiento facial" en las calles de Asunción y zonas del Área Metropolitana. Pese a que la organización TEDIC ha intentado acceder a través de solicitudes de acceso a la información pública presentadas a la información técnica del sistema implementado y los privilegios que respecto a este caben al proveedor privado de la tecnología, a la fecha el Estado amparado en causales de seguridad nacional se ha negado a revelar tal información, en un caso que se encuentra pendiente de revisión por la Corte Suprema por la infracción de derechos fundamentales involucrada.[14]

b) Contratación de empresas de seguridad que ofrecen servicios de vigilancia a clientes privados

Este tipo de medidas se hace común por parte de privados que creen que el sistema público es insuficiente para protegerlos de la delincuencia. Así, directamente contratan y despliegan sistemas de vigilancia de orden tecnológico para incrementar su sensación de seguridad. Uno de los casos más comunes debido a sus bajos costos es la instalación de cámaras de vigilancia fijas o móviles en espacios abiertos o semicerrados pero de circulación pública, como el exterior de edificios, transporte público, espacios comunes de condominios o centros comerciales.

La utilización para fines de seguridad ciudadana por parte de privados de cámaras de vigilancia levanta siempre una tensión entre privacidad y seguridad. Así, por ejemplo, en **Perú** el 2015 el Tribunal Constitucional determinó que "el derecho a la libertad individual de los vecinos no se ve afectado si uno de ellos coloca cámaras de videovigilancia en la puerta de su vivienda".[15]

---

[12] Alguien te mira: así funciona el gigante de las campañas políticas que controla Sosafe. Ciper. 11 de septiembre 2019. https://ciperchile.cl/2019/09/11/alguien-te-mira-asi-funciona-el-gigante-de-las-campanas-politicas-que-controla-sosafe/

[13] Sosafe descarta traspaso de datos personales a empresa controladora que asesora campañas de Chile Vamos. El Desconcierto. 13 de septiembre 2019. https://www.eldesconcierto.cl/2019/09/13/sosafe-descarta-traspaso-de-datos-personales-a-empresa-controladora-que-asesora-campanas-de-chile-vamos/

[14] TEDIC, Quién vigila al vigilante, 16 de septiembre de 2019, https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/

[15] Cámaras de videovigilancia no afectan derecho de vecinos. La Ley. 14 de febrero 2015. https://laley.pe/art/2195/camaras-de-videovigilancia-no-afectan-derecho-de-vecinos-

Algunos de los países de nuestro continente tanto a nivel de reglamentos como de leyes han regulado el uso de la videovigilancia teniendo en cuenta ámbitos de datos personales y privacidad. Así, por ejemplo, en **México**, aunque difieren en cómo se deben llevar a cabo, se exige una serie de elementos comunes que buscan balancear el escrutinio de la vida de las personas en los espacios públicos con la protección de su privacidad, así como el establecimiento de criterios para instalarlas y gestionar las imágenes y sonidos que graban, incluyendo su inalterabilidad, destrucción y el establecimiento de entidades responsables de la gestión de la videovigilancia.[16]

Mientras que en **Argentina** la ley establece condiciones bajo las cuales resulta legítimo el uso y despliegue de las videocámaras, las cuales deben respetar algunas limitaciones con el fin de proteger la privacidad y el uso de los datos personales recogidos en las grabaciones (imagen, voz, etc.). Como dice Carlos Guerrero de Hiperderecho, "esto resulta de vital importancia pues cualquier nueva tecnología que se incorpore, debe respetar estos principios".[17]

No obstante, hay países que aún tienen mucho que avanzar. En **Perú**, por ejemplo, las normas no son claras respecto del tiempo de conservación y el destino de las grabaciones que no son utilizadas por la Policía Nacional o el Ministerio Público. De acuerdo con Hiperderecho: "Solo existen disposiciones genéricas que ordenan el respeto de la Ley de Protección de Datos Personales y ordenan sanciones adicionales para quienes la incumplan, lo que no impide que las grabaciones puedan ser almacenadas indefinidamente, lo que genera un gran peligro de que estas se extravíen, sean alteradas o hurtadas por terceros. Tampoco estás difundidas en el país buenas prácticas en materia de información al usuario sobre sus derechos de cara a la incorporación de sus datos en estas bases de datos".[18]

En noviembre de 2018, se implementó por una cadena de centros comerciales que opera en **Chile**, un sistema piloto y pionero en toda América Latina de cámaras con reconocimiento facial al interior de las dependencias comerciales con el fin declarado de identificar situaciones de flagrancia y prófugos de la justicia.[19] Todos los clientes concurrentes a las dependencias del centro comercial que son capturados por las cámaras de reconocimiento facial dispuestas a su interior son contrastados con una base de datos proporcionada por la Policía de Investigaciones y su identidad es determinada a través de un software provisto por una empresa privada española, respecto al cuál no existe mayor información técnica y de seguridad disponible. La implementación de este sistema de reconocimiento facial constituye un claro tratamiento de datos personales,

---

[16] Arteaga Botello, Nelson. (2016). Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad. *Espiral (Guadalajara)*, *23*(66), 193-238. Recuperado en 30 de septiembre de 2019, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-05652016000200193&lng=es&tlng=es.

[17] Videovigilancia urbana. Carlos Guerrero. 14 de mayo 2019 https://hiperderecho.org/2019/05/videovigilancia-urbana/

[18] Ibidem

[19] Mallplaza. Mallplaza Los Dominicos presenta inédita tecnología de reconocimiento facial como parte de su moderno plan de seguridad, 13 de noviembre 2018, https://www.mallplaza.com/noticias/mallplaza-los-dominicos-presenta-inedita-tecnologia-de-reconocimiento-facial-como-parte-de-su-moderno-plan-de-seguridad

que involucra datos biométricos de carácter sensible, implementado sin consentimiento expreso de sus titulares, ni una autorización legal expresa que regule y establezca condiciones de supervisión de su ejercicio. El resultado, como era de esperarse, es que a pocos meses de su implementación fue revelado que en el 90% de los casos el sistema implementado arrojaba falsos positivos en la identificación.[20] No obstante, el sistema ha continuado operando con la pasividad y complicidad de las autoridades nacionales.

Por su parte, en **Brasil**, el Metro de Sao Paulo ha anunciado un programa para adquirir cámaras de reconocimiento facial a ser implementadas en todo el sistema público concesionado de la ciudad, sin que exista ningún mecanismo de supervisión y control a la fecha.[21]

c) Integración de capacidades de vigilancia privada a sistemas estatales

Un plan representativo de esta tendencia es el que se presentó en octubre de 2018 en Cali, **Colombia**, debido a la falta de fuerzas policiales para cubrir las necesidades de la ciudad. Por eso se pactó una alianza con las empresas de seguridad privada: "La idea es que todas las cámaras que están en puntos críticos de la ciudad puedan estar enlazadas y que los guardas que monitorean esas cámaras pueden alertar a la Policía cuando haya algún evento sospechoso o algún delito se esté presentando", explicó Andrés Villamizar, secretario de Seguridad de Cali.[22]

En la misma línea, a principios del 2019, el gobierno de la ciudad de **México** propuso instalar durante el año 11.100 nuevas cámaras en la vía pública en los 3.600 postes existentes y en otros 100 postes que serán construidos, lo que ampliará a 26.400 el número de cámaras administradas por el gobierno capitalino a través del C5 (centro de gestión de los sistemas tecnológicos de vigilancia y seguridad de la ciudad). Este ambicioso plan incluye "el deseo de interconectar la infraestructura pública con sistemas de videovigilancia privada, como los que operan en centros comerciales, bancos y centros recreativos, o sistemas controlados por las 16 alcaldías de la ciudad, Metro, Metrobús, Secretaría de Obras capitalina y el Estado de México. La idea no es nueva: el Congreso de Yucatán aprobó una ley que regula esta interoperabilidad público y privada en julio de 2018. Si fuera el caso, el C5 podría tener acceso a las 1,190 cámaras de videovigilancia instaladas en el Aeropuerto Internacional de la Ciudad de México".[23]

---

[20] Consejo para la transparencia. CPLT insiste en que reconocimiento facial en mall capitalino es "desproporcionado para el fin que persigue", 14 de marzo de 2019 https://www.consejotransparencia.cl/cplt-insiste-en-que-reconocimiento-facial-en-mall-capitalino-es-desproporcionado-para-el-fin-que-persigue/

[21] Lobel, Fabrício. Metro de São Paulo se apunta al reconocimiento facial, Folha de Sao Paulo, 17 de julio de 2019, https://www1.folha.uol.com.br/internacional/es/saopaulo/2019/07/metro-de-sao-paulo-se-apunta-al-reconocimiento-facial.shtml

[22] La estrategia de la seguridad privada y la Policía para combatir la delincuencia en Cali. Noticias Caracol. 19 de octubre 2018. https://noticias.caracoltv.com/cali/la-estrategia-de-la-seguridad-privada-y-la-policia-para-combatir-la-delincuencia-en-cali

[23] CDMX, vigilancia total; instinto de Big Brother. El Economista. 10 de enero del 2019. https://www.eleconomista.com.mx/opinion/CDMX-vigilancia-total-instinto-de-Big-Brother-20190120-0029.html

Por su parte, en Concordia, **Argentina**, autoridades buscan hacer un registro de todas las cámaras de videovigilancia en la ciudad, ya que las personas que tienen en sus comercios o domicilios particulares, cámaras de videovigilancia que registran el espacio público, "siempre colaboran y acercan el material, por eso es importante que a través de una ordenanza se pueda instrumentar el registro para que la Policía y la Justicia sepan con precisión cuáles son las cámaras, su ubicación. Esto contribuye a acelerar los tiempos, a la vez que le da también una mayor tranquilidad al vecino sobre el uso que se le va a dar a ese registro de imágenes".[24]

III. Marco de derechos humanos

La protección de la privacidad en la era digital es un derecho humano que debe hacer asegurado como un derecho habilitante de muchos otros civiles y políticos, pero también económicos, sociales y culturales. De hecho, tanto la Relatoría Especial para la Libertad de Expresión de la CIDH como la Relatoría Especial para la Privacidad de Naciones Unidas han emitido informes y declaraciones sobre la necesidad de proteger la privacidad en la era digital, basados en instrumentos internacionales que reconocen el derecho a la no interferencia arbitraria sobre la vida privada y familiar de la persona, su domicilio y su correspondencia, o al reconocimiento y respeto a la dignidad, integridad personal o reputación, como la Convención Americana sobre Derechos Humanos en su artículo 11, la Declaración Universal de Derechos Humanos en su artículo 12 y el Pacto Internacional de Derechos Civiles y Políticos en su artículo 17, entre otros.

Todo lo anterior significa que, concretamente, todos los países firmantes de tratados internacionales deben cumplir con una serie de estándares necesarios para velar por la privacidad de las personas. Particularmente, según la Corte Interamericana de Derechos Humanos,[25] esto se traduce a:

> a) el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas; b) el derecho a gobernarse por reglas propias según el proyecto individual de vida de cada uno; c) el derecho al secreto respecto de lo que se produzca en ese espacio reservado con la consiguiente prohibición de divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona; y d) el derecho a la propia imagen.

De forma particular, el Sistema Interamericano de Derechos Humanos (SIDH) ha establecido un test tripartito (legalidad, proporcionalidad y necesidad) para verificar la adecuación al marco interamericano de derechos humanos de las injerencias **estatales o no estatales** en la vida privada mediante las vigilancias en contextos digitales. La legalidad supone que las medidas de vigilancia de los Estados deben estipularse de forma previa a la actuación estatal y debe contener de manera expresa tanto en el sentido formal como material las disposiciones que habiliten la vigilancia. Para la RELE,

---

[24] A través de una ordenanza podrían censar todas las cámaras de video vigilancia en la ciudad. Diario Junio Digital. 22 de agosto 2019. http://www.diariojunio.com.ar/noticia.php?noticia=96697

[25] Relatoría Especial para la Libertad de Expresión (2017). "Estándares para una Internet libre, abierta e incluyente", Comisión Interamerica- na de Derechos Humanos, OEA/Ser.L/V/II CIDH/RELE/INF.17/17. párr. 191.

la necesidad implica que cualquier medida de restricción sea adecuada y suficientemente justificada, así como la proporcionalidad estará dada por el balance entre el objetivo imperioso y necesario, y el impacto de la limitación del derecho individual propuesto.[26]

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.

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, asegurando un más efectivo de los derechos civiles y políticos, pero también derechos económicos, sociales y culturales, tales como un mejor acceso a la educación, la facilitación de acceso a los servicios de salud y seguridad social, así como nuevas oportunidades de trabajo, entre otros. Sin embargo, los servicios y productos generados por las empresas que ofrecen tecnologías de vigilancia constituyen una amenaza para el ejercicio de los derechos económicos sociales y culturales de muchas usuarias por el riesgo de discriminación que ellas conllevan, particularmente, de sectores más vulnerables y tradicionalmente discriminados como mujeres, pueblos indígenas, personas con discapacidad, adultos mayores, personas en situación de calle, personas que padecen enfermedades mentales, comunidades afrodescendientes, y población LGBT+, por mencionar algunos.

El uso discriminatorio de las tecnologías de vigilancia es preocupante desde una perspectiva de política pública, pues muchas de estas tecnologías son precisamente implementadas con la finalidad de fragmentar los espacios públicos, desalentando la protesta pública, la movilidad social y la integración de las ciudades entre grupos pertenecientes a diferentes grupos socioeconómicos. En esta materia, cabe una responsabilidad clara de las empresas en cuanto proveedoras de tecnologías que son utilizadas para la vigilancia. 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.

[26] La construcción de estándares legales para la vigilancia en América Latina. Parte I: Algunos ejemplos de regulación actual en América Latina. Becker, Lara & Canales. 2018. https://www.derechosdigitales.org/wp-content/uploads/construccion-estandares-legales-vigilancia-I.pdf

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,[27] 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.

IV. Cómo responden los marcos legales locales al desafío de los derechos humanos en la regulación de las tecnologías de vigilancia

En su documento "La construcción de estándares legales para la vigilancia en América Latina",[28] Derechos Digitales concluye que, en su análisis de los marcos legales de Argentina, Brasil, Chile, Colombia, Guatemala y México, son pocas las normativas que hacen expresa referencia a los principios de legalidad, proporcionalidad y necesidad. Esto se presenta como altamente problemático pues deja a las personas en indefensión frente al aparataje estatal y privado de vigilancia cuando existe exceso e ilegalidad en su aplicación.

El informe agrega que "varios países de la región carecen de protección judicial previa frente al acceso a ciertos datos, incluidos los datos biométricos (datos personales sensibles), los datos y metadatos retenidos por ISP (entre ellos geolocalización), y la información obtenida mediante uso de televigilancia. Del mismo modo, una revisión judicial posterior (de oficio o a instancias de la contraparte en un eventual procedimiento judicial) es poco habitual".

Agrega que los Estados carecen de una evaluación de impacto y de reglas especiales en la adquisición de estas tecnologías de vigilancia, que tengan en cuenta el efecto sobre el ejercicio de derechos humanos como la privacidad, la libertad de expresión, el derecho a reunión y el derecho a no ser discriminado.

Particularmente, respecto a tecnologías biométricas, un informe hecho por la Asociación por los Derechos Civiles (ADC) que analiza los marcos legales para el uso de datos biométricos de países como Argentina, Colombia, Brasil y México, concluye que, "en general, las normativas incorporan los conceptos sin brindar definiciones, dejando la interpretación –en muchos casos– al libre entendimiento de las entidades que implementan la tecnología biométrica y realizan el tratamiento de los datos. Esto presenta diversos problemas vinculados a la delimitación, uso y procesamiento de los distintos tipos de datos biométricos que pueden ser recolectados, pues ante la

---

[27] Coalición: Transparencia, Derechos Humanos y Participación mediante las TIC, para un mejor Gobierno y Ciudadanía, Recomendaciones para la transparencia y anticorrupción en la adquisición y uso de tecnologías de vigilancia por parte de los Estados americanos, Abril de 2018, 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

[28] Ibidem.

generalidad, los Estados pueden apuntar a una interpretación más abierta en los datos que pueden utilizar para variados fines".[29]

Además, el mismo documento de ADC agrega que "es evidente la falta de poder con el que cuentan las autoridades de protección de datos en cada país para ejercitar el cumplimiento de la ley y evitar abusos en la utilización de los datos biométricos por el Estado y el sector privado".

Asimismo, tecnologías de vigilancia que buscan perfilar a personas (y, en muchos casos, segregarlas con su uso en casos como el de la videoviglancia) impactan el desarrollo de la vida democrática pues dañan el ejercicio "de ciertos derechos ciudadanos en la medida en que se mina la capacidad de las personas para hacer frente a las lógicas de clasificación y tipificación social que se imponen desde los aparatos de poder".[30]

V. Recomendaciones

La capacidad intrusiva de las tecnologías de vigilancia crece exponencialmente. Que el uso de ellas esté en manos privadas, en el contexto de un interés público como es la seguridad ciudadana, implica un reto enorme para políticas públicas que busquen el fortalecimiento de los derechos humanos.

En este sentido, recomendamos:

- Deben desarrollarse reglas especiales que obliguen, tanto al Estado como a privados que implementen tecnologías para la seguridad ciudadana, a analizar el impacto en derechos humanos que pueden producir la puesta en marcha de esos sistemas. De esta manera, se pueden identificar de antemano los riesgos para el ejercicio y goce de derechos como la privacidad, la libertad de expresión, la libertad de asociación, la libertad de reunión, el trato igual ante la ley y la no discriminación. La aplicación de estas reglas especiales permitirían tomar acciones concretas preventivas para mitigar dichos riesgos.

- Los principios de legalidad, necesidad y proporcionalidad debieran ser los parámetros inspiradores de las políticas de vigilancia así como para reglas especiales, tanto para los Estados como para los privados, independientemente de las tecnologías utilizadas. Esta es la forma más concreta para que las políticas de vigilancia sean consistentes con el respeto de los derechos humanos.

- Asimismo, la implementación de estas tecnologías deben contemplar mecanismos de transparencia, rendición de cuentas y control efectivo que

[29] Tu yo digital: Descubriendo las narrativas sobre identidad y biometría en América Latina: los casos de Argentina, Brasil, Colombia y México. ADC. 2019. https://adc.org.ar/wp-content/uploads/2019/06/050-tu-yo-digital-04-2019.pdf

[30] Arteaga Botello, Nelson. (2016). Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad. *Espiral (Guadalajara)*, *23*(66), 193-238. Recuperado en 30 de septiembre de 2019, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-05652016000200193&lng=es&tlng=es.

permitan a la ciudadanía ejercer sus derechos frente a los abusos que se cometan tanto por privados como por agentes estatales. Ello hace necesario revisar las normas que aplican a su adquisición, implementación, uso y control.

- También es imprescindible contar con autoridades independientes que puedan detectar y sancionar el mal uso de los datos o la implementación de sistemas desproporcionados e ilegales acorde a los estándares internacionales de derechos humanos.

- Paticularmente, es preciso establecer controles específicos para el acceso a las bases de datos y su uso para la identificación de personas, por ejemplo, bajo autorización judicial en causas criminales, que a su vez deben fundarse en determinados delitos de mayor gravedad.

- En especial, a la luz de las tecnologías biométricas que comienzan a predominar en la televigilancia y la justificación de su implementación en razones de seguridad pública, tanto Estados como privados deben replantear lo que entienden como "consentimiento informado". Como afirma ADC, “más allá del consentimiento libre e informado, que siempre debe ser exigido, esto no implica que el mismo sea usado como carta blanca o excusa para que estas tecnologías vulneren otros principios claves en el tratamiento de los datos, como es el caso de la finalidad. Es por ello que los estándares mínimos son irrenunciables para el titular de los datos, no pudiendo ser revocados ni cedidos al momento de prestar su consentimiento, siguiendo el principio in dubio pro-titular del dato, teniendo en cuenta que siempre hay una relación desigual de poder entre quien trata el dato y su titular”.[31]

Suscriben:

- Asociación por los Derechos Civiles (ADC) – Argentina
- TEDIC – Paraguay
- Derechos Digitales - América Latina
- Coding Rights – Brasil
- IPANDETEC – Panamá.

[31] Tu yo digital: Descubriendo las narrativas sobre identidad y biometría en América Latina: los casos de Argentina, Brasil, Colombia y México. ADC. 2019. https://adc.org.ar/wp-content/uploads/2019/06/050-tu-yo-digital-04-2019.pdf