Coalición: Transparencia, Derechos Humanos y
Participación mediante las TIC, para un mejor Gobierno y Ciudadanía
Grupo de trabajo: Transparencia y derechos humanos en las
políticas en torno a las tecnologías de vigilancia.
Marzo 2018.
Documento final.

Recomendaciones para la transparencia y anticorrupción en la adquisición y uso de tecnologías de vigilancia por parte de los Estados americanos

I. Introducción

Las organizaciones firmantes de este documento celebran que los Estados americanos se reúnan en torno a un tema fundamental como la «Gobernabilidad democrática frente a la corrupción». Luchar contra toda forma de corrupción es también defender la democracia a través del fortalecimiento de la transparencia, la rendición de cuentas y la fiscalización de la función pública, no solo del Estado para con el Estado, sino también con la activa participación de otros sectores como la sociedad civil y la ciudadanía en general.

La lucha contra la corrupción no puede hacerse sin la cooperación de los diversos sectores de la sociedad; no puede construirse sin el compromiso por la democracia, ni menos con flagrantes violaciones a los derechos humanos.

En este contexto, vemos con preocupación cómo en los últimos años en nuestros países aumentan los casos de corrupción relacionadas con la adquisición de tecnologías de vigilancia. Aquello no es solo un problema de transparencia y rendición de cuentas de las compras públicas (que además alcanzan cifras millonarias), sino que, más grave aún, significa que a través de procesos corruptos y poco transparentes se está adquiriendo tecnología que posibilita la lesión grave de los derechos humanos de la ciudadanía.

Es que, como ha indicado Edison Lanza, Relator Especial para la Libertad de Expresión de la Organización de Estados Americanos (OEA), "tanto a nivel regional como universal se reconoce que las prácticas de vigilancia y la interceptación y recopilación ilícita o arbitraria de datos personales no sólo afectan el derecho a la privacidad y a la libertad de expresión, sino que también pueden ser contrarios a los preceptos de una sociedad democrática".[1]

Es por eso que, en este documento, las organizaciones firmantes hacen un llamado a los Estados Americanos a tomar medidas particulares para luchar contra la corrupción en la adquisición de tecnologías de vigilancia, pues entendemos que más allá de fortalecer la transparencia, aquello implica atender a la tarea urgente de defender la democracia y los derechos humanos.

II. Breves antecedentes sobre las tecnologías de vigilancia y su mercado

Si bien las actividades de vigilancia de los Estados son parte fundamental de su labor de prevención en materia de seguridad pública, en tanto es una de las formas de evitar que sucedan ataques que pongan en peligro las vidas y los bienes de las personas que habitan el suelo de los distintos países, ello nunca puede prestarse como excusa para la vulneración de derechos humanos. No existe verdadera garantía de la seguridad pública sin respeto por los derechos humanos de los ciudadanos de los Estados americanos, cualquier restricción de derechos sólo puede ejecutarse en forma excepcional conforme garantías de debido proceso altamente reconocidas en los sistemas jurídicos de la región, y la adquisición y el uso de la tecnología no puede ser una excepción a tal principio.

[1] Estándares para una Internet libre, abierta e incluyente. Edison Lanza. OEA. 2017. Consultado el 20 de marzo de 2018 en https://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf

Ahora bien, conforme la tecnología avanza y nuestras sociedades se digitalizan, las herramientas de vigilancia se han hecho cada vez más eficientes y 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, en este caso de carácter tecnológico, ha hecho florecer una pujante industria de vigilancia en el mundo.[2]

Así, como reconoce la ONG Hiperderecho del Perú, "las actividades de vigilancia pueden llevarse a cabo a través de una amplia gama de medidas técnicas, incluyendo: la escucha telefónica, la intervención de las comunicaciones electrónicas, la difusión de programas de ordenador maliciosos (malware, spyware) o el control remoto de teléfonos celulares o computadoras con la finalidad de extraer información del vigilado. También existen, técnicas de vigilancia masiva como el monitoreo de datos de comunicaciones o metadatos desde las fibras ópticas de acceso a internet, el acceso a los datos de geolocalización de un usuario, la retención obligatoria de datos, entre otros".[3]

Particularmente, como forma de vigilancia gubernamental, el hackeo[4] presenta amenazas únicas y graves a nuestra privacidad y seguridad. Como reconoce Privacy International, tiene el potencial de ser mucho más intrusiva con la privacidad que cualquier otra técnica de vigilancia.[5] Usando herramientas de hackeo, el Estado aprovecha vulnerabilidades en el software de los aparatos de las personas. Como lo ha analizado la Fundación Karisma de Colombia,[6] el uso de estas herramientas -además de excesivo- es ilegítimo, permitiendo al gobierno acceder de forma remota y secreta a nuestros dispositivos personales y a los datos almacenados en ellos, así como encender el micrófono, la cámara o la tecnología de localización basadas en GPS. Se trata de una intromisión total en la vida íntima de la persona vigilada que permite también a los gobiernos manipular los datos en nuestros dispositivos, incluyendo la plantación o eliminación de datos, o la recuperación de datos que se han eliminado, todo mientras borra cualquier rastro de la intrusión, lo que puede ser fácilmente usado para actividades de corrupción.

A ese contexto actual de tecnologías de vigilancia altamente intrusivas, se suma las prácticas históricas de los Estados respecto a la vigilancia de la ciudadanía en nuestro continente. Los países que sufrieron dictaduras militares en el pasado reciente o que han tenido conflictos armados, cargan con una herencia que, por lo general -y como reconoce la Asociación por los Derechos Civiles de Argentina- implica métodos opacos de vigilancia, recolección desproporcionada de información, secreto excesivo, falta de transparencia y una larga experiencia en violaciones a derechos humanos que han quedado impunes.[7] Esto ha hecho que aún en el presente existan prácticas ligadas a actividades de inteligencia que no están alineadas con una perspectiva amplia de derechos humanos, no tienen adecuado control, y son usualmente fuente de conductas ilegales que terminan violentando derechos de los ciudadanos o debilitando el sistema democrático y sus instituciones.

---

[2] Privacy International launches the Surveillance Industry Index & New Accompanying Report. 2017. Privacy International. Consultado el 20 de marzo de 2018 en https://privacyinternational.org/blog/54/privacy-international-launches-surveillance-industry-index-new-accompanying-report

[3] Vigilancia Estatal de las Comunicaciones y Derechos Fundamentales en Perú. Miguel Morachimo. 2016. Electronic Frontier Foundation & Hiperderecho. Consultado el 20 de marzo de 2018 en https://necessaryandproportionate.org/es/country-reports/peru

[4] "Hackear" es una expresión que identifica una ética que consiste en propiciar el acceso a la tecnología para empoderar a las personas, luego se entendió como la actividad de encontrar vulnerabilidades en sistemas de información, pero esencialmente con la idea de reportarlas y repararlas. Finalmente se empezó a usar en el sentido de buscar vulnerabilidades en sistemas de información y aprovecharlas en forma ilícita. En este documento la expresión "hackear" en este mismo sentido como el uso de herramientas de hackeo por parte del Estado.

[5] Privacy International's oral statement to the Human Rights Council 37th ordinary session. 2018. Privacy International. Consultado el 20 de marzo de 2018 en https://privacyinternational.org/advocacy-briefing/1655/privacy-internationals-oral-statement-human-rights-council-37th-ordinary

[6] Cuando el Estado "Hackea": Análisis de la legitimidad del uso de herramientas de hacking en Colombia. Juan Diego Castañeda. 2015. Fundación Karisma. Consultado el 20 de marzo de 2018 en https://karisma.org.co/cuando-el-estado-hackea-3/

[7] Descubriendo la agenda de ciberseguridad de América Latina. El caso de Argentina. Asociación por los Derechos Civiles. 2015. Consultado el 20 de marzo de 2018 en http://www.adc.org.ar/wp-content/uploads/2015/09/Primera-entrega-Descubriendo-la-Agenda-de-Ciberseguridad-en-Latinoam%C3%A9rica-el-caso-de-Argentina.pdf

Estos antecedentes -tanto la pujante industria de vigilancia, la demanda creciente de los Estados, y un marco institucional poco transparente- hacen urgente que en la agenda de transparencia y la lucha contra la corrupción en nuestro continente se agregue la compra y uso de tecnología de vigilancia, con el fin de evitar el socavamiento de los derechos humanos y la gobernabilidad democrática de los países.

III. Efectos nocivos de la poca transparencia en la adquisición de tecnologías de vigilancia

Lamentablemente, la falta de transparencia y control ciudadano en la adquisición y uso de tecnologías de vigilancia ya muestra diversos efectos nocivos en el continente, entre los cuales se encuentran:

- **Malversación de dineros públicos**

Las tecnologías de vigilancia son productos y servicios de alto valor monetario que solo pocos entes tienen el poder de adquirir. Asimismo, si bien la materia carece de regulación específica en lo concerniente a la adquisición de tecnología, muchas de estas compras están dentro de aquellas reguladas por ley, por lo que, desde una perspectiva normativa al menos, se restringe quién tiene el poder de hacerlo y en qué condiciones.

Sin embargo, las previsiones legales no han sido suficientes ni eficaces por sí solas para evitar que funcionarios públicos tuerzan sus previsiones para poder adquirir y utilizar tecnologías de vigilancia, excediendo el marco autorizado o simplemente ignorando éste. Uno de los casos más importantes de este tipo es el ocurrido en Panamá, pues se calcula que el gobierno del expresidente Ricardo Martinelli -entre el 2009 y el 2014- contrató por 13.5 millones de dólares a las empresas M.L.M. Protection Ltd. y NSO Group para adquirir tecnologías para interceptar las comunicaciones. El negocio ilegal se logró a través del Programa de Ayuda Nacional (PAN), que por cierto nunca se discutió bajo el artículo 67 de la Ley 22 de Contrataciones Públicas de ese país centroamericano.[8] Por tal razón, la Corte Suprema de Justicia de Panamá ha acusado al ex presidente de utilizar fondos públicos para espiar ilegalmente a más de 150 opositores políticos durante su mandato presidencial entre 2009 y 2014.

- **Corrupción en adquisiciones con dinero público**

¿Con qué mecanismos de rendición de cuentas los Estados celebran contratos con los proveedores de tecnología de vigilancia? Los casos en nuestro continente son preocupantes. En México, por ejemplo, se habla de los estrechos lazos de los proveedores más importantes de esta industria con el actual gobierno mexicano.[9] En Chile, en tanto, se han registrado compras de tecnología de vigilancia por parte de las policías locales que han terminado en fracaso debido a fallas del producto, y que además se relacionan con sobrepagos.[10] ¿Cómo se mide y se transparenta de cara al público la eficiencia en el gasto de los recursos y la eficacia de la tecnología a la que ellos se destinan?

- **Adquisiciones ilegales**

Uno de los casos emblemáticos en esta materia es el de México. Una investigación comprobó que por lo menos 16 gobiernos estatales y dependencias federales de ese país pagaron más de 100 millones de pesos mexicanos en los últimos cuatro años a la empresa italiana Hacking Team,

[8] Martinelli gastó más de 10 millones de dólares en espionaje. Telesur. 2015. Consultado el 20 de marzo de 2018 en https://www.telesurtv.net/news/Martinelli-gasto-mas-de-10-millones-de-dolares-en-espionaje-20150115-0057.html
[9] Así creció el proveedor de Pegasus durante el gobierno de EPN. Huffpost. 2017. Consultado el 20 de marzo de 2018 en http://www.huffingtonpost.com.mx/2017/06/26/asi-crecio-proveedor-de-pegasus-durante-el-gobierno-de-epn_a_23002706/
[10] Carabineros pagó US$3,3 millones por equipo para "pinchar" teléfonos: lo instaló y no funcionó. Ida Miranda y Bárbara Partarrieu. 2015. Ciper Chile. Consultado el 20 de marzo de 2018 en http://ciperchile.cl/2015/02/12/carabineros-pago-us33-millones-por-equipo-para-pinchar-telefonos-lo-instalo-y-no-funciono/

una compañía que, bajo la fachada de una empresa de ciberseguridad, vende *software* malicioso a 35 países en el mundo, entre ellos varios señalados por graves violaciones a derechos humanos.

La legalidad de la compra ha sido puesta en duda por diversas organizaciones locales, pues de acuerdo con el Código Nacional de Procedimientos Penales y otras leyes generales, solamente las agencias del Ministerio público y Fiscalías -además de órganos de inteligencia- están facultados para realizar una intromisión de comunicaciones privadas y siempre dentro del marco de una averiguación previa. Pero en la lista de clientes revelada en México aparecen instancias como el Cuerpo de Seguridad Auxiliar Mexiquense o Petróleos Mexicanos que no tienen esas facultades.[11]

- **Espionaje y acoso a activistas, defensores de derechos humanos y periodistas**.

Este tipo de adquisiciones ilegales de tecnologías de vigilancia ponen en duda no solamente los niveles de transparencia y rendición de cuentas de este tipo de compras por parte de los Estados, sino también dejan un manto de dudas sobre quién o quiénes tienen el control de la tecnología y con qué fines la utilizan.

Efectivamente, hay diversos casos en todo el continente donde el uso de tecnologías de vigilancia no resiste ningún control en el marco de la legalidad. Este es el caso, por ejemplo, de cuando estas tecnologías se usan para vigilar sin justificación legal a activistas y organizaciones de la sociedad civil, a periodistas que son incómodos al poder, a poblaciones vulnerables como las indígenas, a actores políticos, etc. Lamentablemente, los ejemplos recientes abundan de espionaje ilegal por tecnologías de vigilancia a opositores políticos, activistas y periodistas en México,[12] Brasil,[13] Panamá,[14] Colombia,[15] Perú,[16] Paraguay,[17] Argentina[18] y Chile,[19] entre tantos otros.

- **Falta de transparencia y rendición de cuentas con información verificable**

Los casos arriba referidos ponen en duda la información proporcionada (en caso de que lo hagan) por los Estados respecto de la adquisición, uso y alcance de las tecnologías de vigilancia que implementan. Hay un mercado opaco hacia el ojo público, prácticamente inauditable por instancias tanto estatales como desde la sociedad civil, reñido con la protección y el fortalecimiento de los derechos humanos de la ciudadanía. La falta de control de las actividades de vigilancia de los Estados hace sospechar de cualquier mecanismo de rendición de cuentas, lo que atenta contra la gobernabilidad y confianza de la ciudadanía con la democracia.

---

[11] México, el principal cliente de una empresa que vende software para espiar. Arturo Angel. Animal Político. 2015. Consultado el 20 de marzo de 2018 en http://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/

[12] Consultado el 20 de marzo de 2018 en https://r3d.mx/gobiernoespia

[13] Salí a cazar equipos de vigilancia en los juegos Olímpicos. Dia Kayyal. Chupadatos. 2016. Consultado el 20 de marzo de 2018 en https://chupadados.codingrights.org/es/sai-para-cacar-equipamentos-de-vigilancia-no-rio-olimpico/

[14] Cronología del caso de escuchas en Panamá por el que detienen a Ricardo Martinelli en EEUU. Acento. 2017. Consultado el 20 de marzo de 2018 en https://acento.com.do/2017/actualidad/8465768-cronologia-del-caso-escuchas-panama-detienen-ricardo-martinelli-eeuu/

[15] Sistemas de vigilancia en Colombia al descubierto. Fundación Karisma. 2015. Consultado el 20 de marzo de 2018 en https://karisma.org.co/sistemas-de-vigilancia-en-colombia-al-descubierto/

[16] DINI: esta es la lista de políticos y empresarios rastreados. 2015. El Comercio. Consultado el 20 de marzo de 2018 en https://elcomercio.pe/politica/gobierno/dini-lista-politicos-empresarios-rastreados-344286

[17] Espionaje a periodista confirma que el Estado intercepta comunicaciones ilegalmente. Maricarmen Sequera. TEDIC. 2016. Consultado el 20 de marzo de 2018 en https://www.tedic.org/espionaje-a-periodista-confirma-que-el-estado-intercepta-comunicaciones-ilegalmente/

[18] El historial de la Argentina sobre privacidad y vigilancia bajo escrutinio en la ONU. ADC Digital. 2016. Consultado el 20 de marzo de 2018 en https://adcdigital.org.ar/2016/06/27/historial-argentina-privacidad-vigilancia-onu/

[19] Poco y nada (o cuánto sabemos realmente sobre cómo nos vigilan). Vladimir Garay. Derechos Digitales. 2017. Consultado el 20 de marzo de 2018 en https://www.derechosdigitales.org/11446/poco-y-nada-o-cuanto-sabemos-realmente-sobre-como-nos-vigilan/

IV. Recomendaciones a los Estados Americanos

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.

En este contexto, y debido al especial régimen legal que las actividades de vigilancia requieren en los Estados, y dada la afectación de derechos humanos que tales actividades implican, es importante proponer una serie de medidas particulares que estimamos debieran incorporarse en la gobernabilidad de los Estados para combatir la corrupción en este ámbito:

- **Transparentar información sobre la adquisición de tecnología de vigilancia**

Una de las formas más potentes de luchar contra la corrupción en la adquisición de tecnología de vigilancia, y en su uso descontrolado, es fortalecer todos los mecanismos de transparencia en el proceso de adquisición.

Respecto a la adquisición de tecnologías de vigilancia, y debido al peligroso potencial intrínseco de ellas para violar los derechos humanos, los Estados deben definir marcos legales claros y específicos de quiénes pueden realizar estas compras y bajo qué supervisión y condiciones, así como asegurar mecanismos de fiscalización independiente, transparencia y rendición de cuentas a la ciudadanía.

Además del marco legal, y debido a que la contratación pública se ha identificado como una de las actividades gubernamentales más vulnerable a la corrupción, los Estados Americanos deben fortalecer su compromiso con los principios de publicidad, transparencia y libre concurrencia en los procesos de contrataciones públicas cuando se trata de tecnologías de vigilancia. Todos los ciudadanos y ciudadanas deben ser capaces de monitorear las compras y contrataciones de servicios al respecto.

Así, debe haber difusión pública de información relativa a procedimientos de contratos de este tipo de servicios, e información pertinente y oportuna sobre su adjudicación, dando prioridad al principio de máxima divulgación, y acotando a su mínima expresión la disposición, interpretación y aplicación de las figuras del secreto y la confidencialidad de la información.

A esto se suma que los criterios de selección de proveedores deben ajustarse a un estándar de probidad y compromiso irrestricto con los derechos humanos: las empresas no deben presentar antecedentes de corrupción previa ni deben estar relacionadas -directa o indirectamente a través de sus intermediarios- en venta de tecnología de vigilancia que haya sido utilizada para violar los principios democráticos, los derechos humanos, entre ellos en particular la privacidad, la libertad de expresión y de reunión o asociación.

Asimismo, los Estados deben avanzar firmemente en un claro conjunto de valores y normas éticas, expresado en un código de conducta modelo para los responsables de contratación, que defina especiales restricciones y prohibiciones respecto a la adquisición de tecnologías de vigilancia (por ejemplo, declaraciones de interés).

- **Transparentar información sobre el uso de tecnología de vigilancia**

Actualmente, la opacidad en la que operan estos mecanismos es, indudablemente, una excusa para que se hagan compras ilegales y usos no autorizados. Como ha señalado la Red en Defensa de los Derechos Digitales de México, R3D, “si bien las medidas de transparencia por sí mismas no inhiben todos los riesgos de abuso, el conocimiento de estadísticas y otras particularidades respecto de cómo es que el Estado hace uso de las medidas de vigilancia, permite a la ciudadanía conocer el volumen y

alcance de estas medidas y permite informar la discusión pública sobre la pertinencia y las condiciones que deben establecerse para permitir este tipo de invasiones a la privacidad".[20]

Los Estados Americanos se encuentran vinculados en la actualidad por múltiples obligaciones internacionales vigentes respecto al uso de las tecnologías de vigilancia. Por ejemplo, en la resolución "El derecho a la privacidad en la era digital", adoptada por consenso por los miembros de la Asamblea General de la ONU el 18 de diciembre de 2013, se recomienda a los Estados establecer o mantener "mecanismos nacionales de supervisión independiente y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado".[21]

Asimismo, diferentes grupos de la sociedad civil, la industria y expertos internacionales en la materia han elaborado y promovido los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, dentro de los cuales se encuentra el Principio de Transparencia: "los Estados deben ser transparentes respecto del uso y alcance de las medidas de vigilancia de las comunicaciones que implementen, debiendo publicar, como mínimo, información comprehensiva relativa al número de solicitudes aprobadas y rechazadas, un desglose de las solicitudes por proveedor de servicios, por autoridad investigadora, el tipo de medidas utilizadas, su objetivo y el número de personas afectadas por cada una, entre otros".[22]

- **Control democrático de las actividades de vigilancia**

La adquisición y uso de tecnologías de vigilancia debe ser sometida al más estricto orden de legalidad (debido a las consecuencias que tiene su uso en los derechos humanos de las personas), así como al control democrático que permita la construcción de confianza de la ciudadanía con el Estado.

Como pone en evidencia una declaración pública de un grupo de organizaciones de la sociedad civil de América Latina, "debido a los bajos estándares de control legal en la adquisición y uso de las tecnologías de vigilancia en la región, se necesita una discusión abierta en los Congresos nacionales acerca de las leyes que rigen y regulan las actividades de vigilancia, sometidas al escrutinio público. Ante la posibilidad técnica de que estas actividades pongan en riesgo derechos humanos, estas legislaciones deben reflejar los estándares más altos y sujetar las acciones de los organismos de inteligencia a la autorización previa de un organismo judicial imparcial e independiente".[23]

En particular, cinco recomendaciones a los Estados Americanos pueden ser pertinentes al respecto:

1. Establecer con claridad y precisión las autoridades facultadas, las circunstancias y los procedimientos para intervenir comunicaciones privadas, incluyendo el acceso a metadatos de comunicaciones, así como para llevar a cabo la localización geográfica en tiempo real de equipos de comunicación.

2. Establecer explícitamente la necesidad de contar con una autorización judicial previa para llevar a cabo medidas de vigilancia, salvo casos de emergencia en los que el control judicial deberá ser inmediato.

3. Regular la adquisición y operación de herramientas de vigilancia, especialmente el uso de malware para vigilancia, limitando su uso con base a los principios de necesidad y proporcionalidad,

---

[20] El estado de la vigilancia fuera de control. R3D. 2016. Consultado el 20 de marzo de 2018 en https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf
[21] ONU. Asamblea General. Resolución aprobada por la Asamblea General el 18 de diciembre de 2013. 68/167. El derecho a la privacidad en la era digital. A/RES/68/167. 21 de enero de 2014.
[22] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Disponibles. Consultado el 20 de marzo de 2018 en https://necessaryandproportionate.org/es/necesarios-proporcionados
[23] Sociedad Civil de América Latina rechaza software espía de Hacking Team. Vladiir Garay. Derechos Digitales. 2015. Consultado el 20 de marzo de 2018 en https://www.derechosdigitales.org/9081/sociedad-civil-de-america-latina-rechaza-software-espia-de-hacking-team/

así como garantizar que existan registros de los equipos, licencias y capacidades adquiridas. Debe garantizarse la existencia de registros que identifiquen a los funcionarios capacitados y autorizados para utilizar dichas herramientas de vigilancia, así como a la cadena de custodia respecto del proceso de selección de objetivos, operación del sistema y procesamiento de inteligencia obtenida a través de dichas herramientas.

4. Otorgar facultades de fiscalización y supervisión de los sistemas de vigilancia a una autoridad independiente. Debe garantizarse a estas autoridades acceso irrestricto a cualquier información o instalación necesaria para llevar a cabo su labor de fiscalización.

5. Reconocer el derecho de toda persona a ser notificado de injerencias estatales en su vida privada. Dicha notificación solamente podrá ser diferida cuando de manera demostrable esa notificación obstaculice seriamente una investigación o ponga en riesgo la vida o integridad física de una persona.

- **Compromiso con la investigación independiente**

Como se observó en el marco del 167 periodo de sesiones de la Comisión Interamericana de Derechos Humanos, organizaciones de la sociedad civil ven con especial preocupación la falta de voluntad de algunos estados para concurrir a investigaciones independientes respecto a la adquisición y uso de tecnologías de vigilancia, lo que favorece la impunidad y el quebranto de la gobernabilidad democrática.[24]

Los Estados deben suministrar los mecanismos de rendición de cuentas en la adquisición y uso de tecnologías de vigilancia, otorgando todas las facilidades para el acceso y uso de la información por parte de la ciudadanía. Así también, los Estados deben comprometer su voluntad política para una investigación independiente, transparente y eficiente cuando haya denuncias de corrupción, compra ilegal y uso indebido de las tecnologías de vigilancia.

- **Estimular un mercado transparente y apegado a los derechos humanos**

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.

Por ejemplo, en el 2011, la Unión Europea[25] aprobó una resolución para prohibir las ventas en el extranjero de sistemas que monitorean llamadas telefónicas y mensajes de texto, o brindan vigilancia específica por Internet, si se utilizan para violar los principios democráticos, los derechos humanos o la libertad de expresión. Asimismo, existe el Arreglo de Wassenaar sobre control de exportaciones de Armas Convencionales y bienes y tecnología de Doble Uso[26] que, a partir de enero de 2015, restringe la exportación de software intrusivo.

Los Estados del continente productores de este tipo de tecnologías de vigilancia deben buscar imitar y/o plegarse a este tipo de acuerdos para asegurar que la producción y la adquisición de la tecnología de vigilancia por los Estados se enmarque en el respeto de los derechos humanos. Por su parte, lo Estados compradores de este tipo de vigilancia, deben exigir a sus proveedores -directos o

[24] "La PGR parece determinada a que el caso #GobiernoEspía quede impune", denuncia R3D ante la CIDH. R3D. 2018. Consultado el 20 de marzo de 2018 en https://r3d.mx/2018/02/28/la-pgr-parece-determinada-a-que-el-caso-gobiernoespia-quede-impune-denuncia-r3d-ante-la-cidh/

[25] EU Parliament Takes the First Step to Prevent Sales of Surveillance Equipment Used to Violate Human Rights. Cindy Cohn. EFF. 2011. Consultado el 20 de marzo de 2018 enhttps://www.eff.org/deeplinks/2011/10/eu-parliament-takes-first-step-bans-sales

[26] Régimen intergubernamental utilizado para definir y determinar qué productos deben ser sujetos a licencia para exportarlos y fomentar la seguridad internacional.

intermediarios- cumplir con estándares internacionales de respeto a derechos humanos y de probidad en sus transacciones, como los estándares proporcionados por las Naciones Unidas para el respeto de los derechos humanos por parte de las empresas.[27]

:::

Grupo de trabajo coordinado por Paz Peña.

Firman:
- IPANDETEC - Panamá
- Hiperderecho - Perú
- TEDIC - Paraguay
- Derechos Digitales – América Latina
- Fundación Karisma – Colombia
- R3D - México
- Coding Rights - Brasil
- Asociación por los Derechos Civiles - Argentina
- Fundación Datos Protegidos - Chile

[27] UN "Protect, Respect and Remedy" Framework and Guiding Principles. Consultado el 20 de marzo de 2018 https://business-humanrights.org/en/un-secretary-generals-special-representative-on-business-human-rights/un-protect-respect-and-remedy-framework-and-guiding-principles