

Día Internacional de los Derechos Humanos – Declaración conjunta

Vigilancia, seguridad y privacidad: llamamiento para que Uruguay adopte estándares de derechos humanos

En el marco del Día Internacional de los Derechos Humanos 2014, las organizaciones firmantes de esta declaración queremos llamar la atención sobre la necesidad de que el Estado adopte estándares que garanticen el respeto a los derechos humanos, la transparencia y la rendición de cuentas frente a la implementación de sistemas de vigilancia en el marco de su política de seguridad.

A nivel global la irrupción de las nuevas tecnologías de la comunicación y la información han creado un fuerte desafío en materia de derechos humanos. Por un lado, la masificación de internet y del uso de la tecnología en la vida cotidiana ha contribuido a garantizar la libertad de expresión y el acceso a la información, el conocimiento y la cultura en formas antes no concebidas.

En particular, Uruguay ha avanzado en el reconocimiento de nuevos derechos en los últimos años. En el plano de derechos y nuevas tecnologías, ha sancionado una ley de software libre y formatos abiertos que promueve el acceso a la información y al conocimiento. También ha tomado medidas en respuesta a la vigilancia y el espionaje masivos de Estados Unidos, en especial con el decreto sobre ciberseguridad, que protege los datos de los ciudadanos gestionados por el Estado respecto del espionaje de gobiernos extranjeros. En cuanto a los derechos de acceso a la cultura y al conocimiento, el parlamento uruguayo se encuentra estudiando un Proyecto Ley que prevé la despenalización de las descargas sin fines de lucro y sin intención de perjudicar al autor, conjuntamente con una serie de excepciones a los derechos de autor para educación y bibliotecas. Estas excepciones legitiman actividades relacionadas con la digitalización y distribución de obras para su preservación o puesta a disposición en colecciones digitales con fines de enseñanza, investigación y préstamo controlado.

Sin embargo, tal como lo ha señalado recientemente el Alto Comisionado de las Naciones Unidas para los Derechos Humanos, “en la era digital, las tecnologías de la comunicación también han aumentado la capacidad de los gobiernos, las empresas y los particulares para realizar actividades de vigilancia, interceptación y recopilación de datos”.¹ Esta circunstancia determina que “las plataformas tecnológicas de las que depende crecientemente la vida política, económica y social a nivel mundial no solo son vulnerables a la vigilancia en masa, sino que en realidad pueden facilitarla”.²

1

A/HRC/27/37, párr.2

2

Ibídem.

Frente a la creciente preocupación mundial por resguardar los derechos humanos en la era digital, en diciembre de 2013 la Asamblea General de Naciones Unidas aprobó la resolución 68/167 sobre el derecho a la privacidad en la era digital. La resolución afirmó que los derechos de las personas también deben estar protegidos en Internet, y exhortó a todos los Estados a que respeten y protejan el derecho a la privacidad en las comunicaciones digitales. La resolución instó a todos los Estados a examinar sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, haciendo hincapié en la necesidad de que los Estados velen por el pleno y efectivo cumplimiento de sus obligaciones en virtud del derecho internacional de los derechos humanos. Recientemente, en noviembre de 2014, retomando el pronunciamiento anterior, la Asamblea General de la ONU reafirmó mediante resolución³ que los mismos derechos humanos que las personas tienen “fuera de línea” deben ser garantizados “en línea”, incluyendo el derecho a la privacidad.

Otros antecedentes relevantes de pronunciamientos que promueven estándares que garantizan la protección de los derechos humanos frente a la implementación de sistemas de vigilancia a nivel global han sido:

- [Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión](#)⁴, emitida por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA y la Relatoría Especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de opinión y de expresión (2013).
- Conocidos como [los principios de Tshwane](#), un conjunto de más de 500 expertos de todo el mundo acordaron promover una serie de Principios globales sobre seguridad nacional y acceso a la información pública⁵ (2013).
- [Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones](#)⁶. Un grupo de expertos a nivel global elaboraron un documento que establece la necesidad de que dicha actividad se realice bajo condiciones de legalidad, necesidad y proporcionalidad.

3

(A/C.3/69/L.26/Rev.1)

4

<http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927>

5

<http://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf>

6

<https://es.necessaryandproportionate.org/text>

“El Guardián”

Mientras estas acciones y pronunciamientos sucedían a nivel internacional y regional, el Gobierno de Uruguay, en línea con lo que ha venido ocurriendo en muchos otros países, avanzó en secreto en la compra del software de vigilancia “El Guardián”, sin ningún tipo de control parlamentario y prácticamente sin brindar casi ninguna información sobre la implementación del sistema que permitiría espiar llamadas telefónicas y correos electrónicos.

El proceso de su adquisición tomó estado público a través del [artículo difundido por el diario El País en junio de 2013](#)⁷ y muy poco se ha avanzado desde entonces en el acceso a información relevante para la sociedad respecto a las características del software y su implementación.

A la falta de una política proactiva de información que permita conocer efectivamente a la ciudadanía las garantías que se han dispuesto, se suma la clasificación de toda información relativa al nuevo sistema. Las autoridades se han limitado a anunciar que El Guardián será utilizado sólo mediante autorización judicial, cuestión necesaria pero no suficiente en el marco de los estándares de ddhh presentes en la materia.

El estado de situación actual deja dudas acerca de cómo funcionará El Guardián y ofrece pocas certezas a la sociedad en cuanto a su manejo por parte de las autoridades. Existen preguntas clave a responder tales como:

- *¿Cuándo comenzará efectivamente a operar “El Guardián”?*
- *¿Bajo qué marco regulatorio operará esta nueva herramienta?*
- *¿Quiénes serán los encargados de gestionar y controlar esta herramienta?*
- *¿Cómo se garantizan los derechos de las personas sujetas a vigilancia?*⁸

En octubre de 2014 se hizo público a través de la prensa que desde el Ministerio del Interior se continuaría avanzando para la implementación del sistema en el mes de enero próximo. Asimismo se dio cuenta de la existencia de un decreto del Ministerio de Economía y Finanzas que establecería exoneraciones tributarias a efectos de que las empresas de telecomunicaciones adquirieran la tecnología necesaria para la implementación del software. Dicho decreto habría sido declarado reservado e incluiría, según informó [el diario El](#)

7

<http://www.elpais.com.uy/informacion/gobierno-compro-guardian-espiar-llamadas-correos.html>

8

Para ver una descripción del estado de situación actual en referencia a este tema puede consultarse el siguiente documento “*En Penumbas: Vigilancia, Seguridad y Derechos Humanos en Uruguay*” disponible en <http://www.giswatch.org/en/country-report/communications-surveillance/uruguay> (versión en inglés). Un post en español ha sido publicado en <http://www.digitalrightslac.net/es/el-guardian-que-vigila-a-los-ciudadanos/>

[Observador](#)⁹, un protocolo para instrumentar la operativa entre el Ministerio del Interior y las empresas de telecomunicaciones ante solicitudes de vigilancia autorizadas por el Poder Judicial.

En este marco, el 15 de octubre el Centro de Archivos y Acceso a la Información Pública (CAinfo) presentó una solicitud de acceso a la información pública en el marco de la ley 18.381 solicitando tanto al Ministerio de Economía como al del Interior, la entrega de una copia del referido decreto y del protocolo. Las solicitudes no han sido respondidas por ninguno de los dos organismos, en contravención del procedimiento y de los plazos legales.

Las organizaciones firmantes exhortamos al Ministerio del Interior y al Poder Ejecutivo a garantizar el acceso a la información por parte de la población sobre el nuevo sistema de vigilancia y a adecuar su implementación en el marco de los siguientes estándares internacionales:¹⁰

- Los derechos a la privacidad y a la libre circulación del pensamiento e información se encuentran protegidos por el derecho internacional de los derechos humanos; éste prohíbe las injerencias arbitrarias o abusivas en la vida privada, incluidas las comunicaciones y por tanto, reconoce el derecho de las personas a obtener la protección del Estado contra este tipo de injerencias.
- Si bien de acuerdo a los estándares internacionales la protección de la seguridad nacional puede justificar el uso excepcional de vigilancia en las comunicaciones privadas, este tipo de medidas puede constituir un acto particularmente invasivo que afecta seriamente el derecho a la privacidad y la libertad de pensamiento y expresión. En consecuencia, los Estados deben garantizar que la intervención, recolección y uso de información personal estén claramente autorizadas por ley, a fin de proteger a las personas contra interferencias arbitrarias. La ley deberá establecer límites respecto a la naturaleza, alcance y duración de este tipo de medidas; así como las razones para ordenarlas, las autoridades competentes para autorizarlas, ejecutarlas y supervisarlas y los mecanismos legales para su impugnación.
- Dada la importancia del ejercicio de los derechos en juego para el sistema democrático, la ley debe autorizar el acceso a las comunicaciones y a datos

9

<http://www.elobservador.com.uy/noticia/289757/el-guardian-espiara-desde-enero-mails-y-celulares/>

10

En base a la Declaración Conjunta sobre Programas de Vigilancia y su impacto en la libertad de expresión, Relatoría Especial de las Naciones Unidas para la protección y promoción del derecho a la libertad de opinión y expresión y Relatoría Especial de la CIDH sobre Libertad de Expresión RELE.

personales sólo en las circunstancias más excepcionales definidas en la legislación y en base a los principios de necesidad y proporcionalidad.¹¹

- Cuando se invoque la seguridad como razón para restringir otros derechos humanos, la ley deberá especificar claramente los criterios que deban aplicarse para determinar los casos en que este tipo de medidas resultan legítimas y sólo deberán autorizarse cuando exista un riesgo cierto respecto de los intereses protegidos, y cuando a la vez este daño sea superior al interés general de la sociedad en función de mantener el derecho a la privacidad y a la libertad de expresión del pensamiento y circulación de información.
- La entrega de la información debe ser monitoreada por un organismo de control independiente y contar con garantías suficientes de debido proceso y supervisión judicial.
- Las leyes deben asegurar que el público pueda acceder a información sobre los programas de vigilancia de comunicaciones privadas, su alcance y los controles existentes para garantizar que no puedan ser usados de manera arbitraria. En consecuencia, los Estados deben difundir, por lo menos, información relativa al marco regulatorio de los programas de vigilancia; los órganos encargados para implementar y supervisar dichos programas, los procedimientos de autorización, de selección de objetivos y manejo de datos, así como información sobre el uso de estas técnicas, incluidos datos agregados sobre su alcance. Los Estados deben establecer mecanismos de control independientes capaces de asegurar transparencia y rendición de cuentas sobre estos programas.
- Bajo ninguna circunstancia, los periodistas, integrantes de medios de comunicación o miembros de la sociedad civil que tengan acceso y difundan información reservada sobre este tipo de programas de vigilancia, por considerarla de interés público, pueden ser sometidos a sanciones ulteriores.

11

Al respecto, el Alto Comisionado de Naciones Unidas para los DDHH ha sostenido: “Para comenzar, toda limitación a los derechos a la privacidad reflejados en el artículo 17 debe estar prevista en la ley, y la ley debe ser lo suficientemente accesible, clara y precisa para que una persona pueda leerla y saber quién está autorizado a realizar actividades de vigilancia de datos y en qué circunstancias. La limitación debe ser necesaria para alcanzar un objetivo legítimo, así como proporcional al objetivo y la opción menos perturbadora de las disponibles. Por otra parte, debe demostrarse que la limitación impuesta al derecho (una injerencia en la vida privada, por ejemplo, con el fin de proteger la seguridad nacional o el derecho a la vida de otras personas) tiene posibilidades de alcanzar ese objetivo. Es responsabilidad de las autoridades que deseen limitar el derecho demostrar que la limitación está relacionada con un objetivo legítimo. Además, las limitaciones al derecho a la privacidad no deben vaciar el derecho de su esencia y deben ser compatibles con otras normas de derechos humanos, incluida la prohibición de la discriminación. Si la limitación no cumple esos criterios, es ilegal y/o la injerencia en el derecho a la privacidad es arbitraria” (A/HRC/27/37, párr. 23).

Las organizaciones firmantes llamamos al Estado uruguayo a establecer un diálogo que asegure la adopción de estos estándares por parte de todos los actores vinculados a la implementación de El Guardián. De igual forma instamos al Estado uruguayo a iniciar un diálogo para la construcción de mecanismos de gobernanza y control democrático de este tipo de herramientas que ayude a construir un Uruguay respetuoso de los derechos humanos en la era digital.

Amnistía Internacional Sección Uruguay

Asociación de Bibliotecólogos del Uruguay

Centro de Archivos y Acceso a la Información Pública – CAinfo

Cotidiano Mujer

Creative Commons Uruguay

Datos, Transparencia y Acceso a la Información – DATA Uruguay

Instituto de Estudios Legales y Sociales del Uruguay – IELSUR

Proderechos