COORDINADORA
DERECHOS
HUMANOS
PARAGUAY

DERECHOS HUMANOS
PARAGUAY 2016

DERECHOS HUMANOS
PARAGUAY 2016

Edita
© Coordinadora de Derechos Humanos del Paraguay (Codehupy)
Capítulo Paraguayo de la Plataforma Interamericana de Derechos Humanos
Democracia y Desarrollo (PIDHDD)
Callejón 9, N° 354, entre Tte. Rodi y Dr. Facundo Insfrán,
barrio Dr. Gaspar Rodríguez de Francia. Asunción – Paraguay
codehupy@codehupy.org.py / www.codehupy.org.py

Equipo Editor:
Coordinación General: *Oscar Ayala Amarilla*
Dirección Académica: *Rodrigo Villagra Carron*
Edición: *Paulo César López*
Equipo Académico: *Rodrigo Villagra Carron, Rosa Posa Guinea, Mario Barrios Cáceres y Karina Cuevas*
Corrección: *Rubén Romero*
Secretaría: *Cecilia Fernández*
Revisión final: *Rubén Romero y Cecilia Fernández*
Proyecto Gráfico e ilustración: *Juan Heilborn*
Diagramación: *Rossana Paniagua - Damián Acosta*

Impresión: *AGR S.A. Servicios Gráficos*
Primera Edición, *diciembre 2016*
Tirada: *2.000 ejemplares*

El uso de un lenguaje no sexista es un interés de la Codehupy, por lo que el criterio editorial ha sido nombrar en masculino y en femenino cuando corresponda. Se ha buscado utilizar un lenguaje que no discrimine a ningún grupo humano, particularmente a las personas con discapacidad, viviendo con VIH y Sida, pueblos indígenas, afroparaguayos y afroparaguayas, de orientaciones e identidades sexuales diversas, las feministas y aquellas organizaciones que trabajan con ellas, así como la reivindicación del guaraní como idioma oficial y el reconocimiento de las diversidades culturales.

La elaboración, la edición e impresión de este material fueron posibles gracias a la cooperación y el apoyo de Diakonia –Gente que cambia el mundo– y ASDI; Rainforest Foundation Norway (RFN); Obra Episcopal MISEREOR; International Work Group for Indigenous Affairs (IWGIA); Oxfam en Paraguay; Oficina de la asesora en derechos humanos para Paraguay del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR); Fondo de Población de las Naciones Unidas (UNFPA).

¿Cómo citar un artículo de este informe?
Autor/a del artículo (2016) "Título del artículo", en: Coordinadora de Derechos Humanos del Paraguay *Yvypóra Derécho Paraguáipe – Derechos Humanos en Paraguay 2016*. Asunción: Codehupy, pp. [Página de inicio]-[Página de fin].

EL DESAFÍO DEL CUMPLIMIENTO DE LOS DERECHOS HUMANOS EN INTERNET

DERECHOS DIGITALES

Maricarmen Sequera y Jazmín Acuña

TECNOLOGÍA Y COMUNIDAD (TEDIC)

INTRODUCCIÓN

Internet es un espacio donde se ejercen y disputan derechos. El acceso a la información, al conocimiento, el ejercicio de la libre expresión, nuevas oportunidades de inclusión económica, son solo algunos de los avances que suponen la red y las nuevas tecnologías. Pero con estos avances también se han dado retrocesos en el cumplimiento de los derechos humanos. En 2014, la Oficina del Alto Comisionado de Naciones Unidas para los Derechos Humanos señaló que "así como estas tecnologías facilitan la vida y están al alcance de todos, igualmente se encuentran a disposición de los gobiernos, para los cuales conducir actividades de vigilancia, censuras a la población nunca fue más sencillo, barato y eficiente" (United Nations, 2014).

Las revelaciones del informante Edward Snowden confirmaron la existencia de programas nacionales e internacionales dirigidos por la Agencia Nacional de Seguridad (NSA) de EEUU destinados a vigilar de forma masiva las comunicaciones privadas de millones de usuarios de internet. Sus revelaciones son cruciales porque muestran el poder que pueden acumular los Estados, en asociación con las empresas, a través de las nuevas tecnologías y los abusos que pueden cometer.

En la historia nacional, el Archivo del Terror es el antecedente más grave de vigilancia estatal. Este hallazgo evidenció lo que es capaz un gobierno cuando no está controlado por autoridades judiciales imparciales e independientes, órganos de supervisión pública autónomos y por el público en general. Pero la transición a la democracia no ha eliminado aún viejas prácticas propias de gobiernos autoritarios. En todo caso, los mecanismos de vigilancia solo se han renovado y optimizado.

En los últimos años, varias investigaciones académicas y periodísticas (Rolón y Sequera, 2016) dieron cuenta de que el Estado paraguayo ha adquirido tecnologías para la vigilancia, o lo que se conoce como software malicioso (malware), sin regulaciones ni control alguno. Estas adquisiciones siguen la tendencia mundial en vigilancia digital de las telecomunicaciones, siempre bajo la excusa de la seguridad nacional[1].

Por esta razón, es necesario poner atención a los derechos que el Estado paraguayo puede vulnerar con estas nuevas herramientas, e implementar mecanis-

1 En Paraguay, la Ley Nº 5241/14 señala que los procedimientos de obtención de información establecidos en este título solo se podrán aplicar cuando los órganos e instituciones del Sistema Nacional de Inteligencia (SINAI) no puedan obtener dicha información por fuentes abiertas. La información a ser obtenida debe ser estrictamente indispensable para el cumplimiento de los objetivos estatales de resguardar la paz y seguridad nacional, la estabilidad institucional, la protección del pueblo de amenazas de terrorismo, el crimen organizado, el narcotráfico y la defensa del régimen democrático constitucionalmente consagrado (artículo 24). Tales procedimientos incluyen "a) La intervención de las comunicaciones telefónicas, informáticas, radiales y de la correspondencia en cualquiera de sus formas; b) La intervención de sistemas y redes informáticos; c) La escucha y grabación electrónica, incluyendo la audiovisual, y d) La intervención de cualesquiera otros sistemas tecnológicos destinados a la transmisión, almacenamiento o procesamiento de comunicaciones o información" (artículo 25).

mos para evitar abusos de poder, especialmente cuando se trata de derechos que están garantizados y reconocidos en la Constitución paraguaya como también en los instrumentos internacionales ratificados por el Estado.

MARCO JURÍDICO

La Declaración Universal de Derechos Humanos (ONU, 1948) contempla derechos que son afectados con las tecnologías a disposición del gobierno. Cabe citar entre los especialmente vulnerables el derecho a la privacidad (art. 12), al debido proceso (art. 10), el respeto a la opinión, la libertad de expresión y de prensa (art. 19). Pero no son los únicos. Además peligran otros derechos fundamentales como la libertad de reunión, asociación (art. 20) y el acceso a la información (art. 19) de todas las personas sin distinción alguna de edad, género, clase social y/o económica.

A continuación citamos algunas legislaciones, políticas y hechos que evidencian los desafíos a los que se enfrenta la ciudadanía, como usuaria de internet, para el pleno cumplimiento de sus derechos en el entorno digital.

El derecho a la privacidad es reconocido en la Constitución Nacional como un derecho general a la vida privada o a la intimidad (art. 33). También está protegido con múltiples derechos específicos: el derecho a la inviolabilidad de las comunicaciones (art. 36); el derecho a la protección de datos personales[2] y la garantía de hábeas data (art. 135).

Existen leyes penales[3] y de carácter administrativo[4] que refuerzan la protección de este derecho y sancionan conductas ilegales, salvo que sean autorizadas previamente por orden judicial justificada y en cumplimiento del debido proceso. Estas regulaciones se centran en aquello que tiene que ver con la vigilancia de las comunicaciones, que comprende "monitorear, interceptar, recoger, analizar, usar, preservar, guardar, interferir u obtener información que incluya o refleje las comunicaciones pasadas, presentes o futuras de una persona, se derive o surja de ellas" (Ferrajoli, 1995).

2 Artículo 1 de la Ley Nº 1682/01, modificada por Ley Nº 1969/02, regula el tratamiento de los datos de carácter privado.

3 El Código Penal, Ley N° 1160/97 artículo 146 Violación del Secreto de Comunicación y Código Procesal Penal, artículo 198 Intercepción y secuestro de correspondencia, artículo 199 Apertura y examen de correspondencia, artículo 200 Intervención de comunicaciones y artículo 228 Informes.

4 La Ley N° 642/95 de Telecomunicaciones, en su artículo 89, establece la inviolabilidad del secreto de la correspondencia realizada por los servicios de telecomunicaciones y del patrimonio documental, salvo orden judicial y el artículo 90 establece las prohibiciones que tal inviolabilidad conlleva, por ejemplo de abrir, sustraer, interferir, cambiar texto, desviar curso, publicar, usar, tratar de conocer o facilitar que persona ajena al destinatario tenga conocimiento de la existencia o el contenido de comunicaciones confiadas a prestadores de servicios. El Decreto del Poder Ejecutivo Nº 14.135/96 en su artículo 9 indica las acciones por las cuales se atenta contra la inviolabilidad y el secreto de las telecomunicaciones.

El derecho a la privacidad protege tanto el contenido como otros datos propios del proceso técnico de la comunicación como los "metadatos" o datos de tráfico, entendidos estos como "el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones"[5]. Por esto, la Corte Interamericana de Derechos Humanos (Corte IDH) emitió un fallo que otorga a los metadatos de las llamadas telefónicas el carácter de inviolables[6].

Asimismo, en este 2016, durante el Examen Periódico Universal (EPU), el Estado paraguayo se comprometió a cumplir las recomendaciones sobre la privacidad y el uso de la tecnología[7] para la adopción de medidas necesarias a fin de que las actividades de vigilancia estén acordes a los principios internacionales de derechos humanos.

SITUACIÓN DEL DERECHO

Existen iniciativas y normativas vigentes que ponen en riesgo la privacidad de las personas a través de la interceptación y recolección de la información que generan sus comunicaciones. Un ejemplo de ello es la Ley Nº 4.868/13 de Comercio Electrónico. En su artículo 10, dicha ley dispone que las empresas proveedoras de internet en Paraguay y proveedores de servicios de alojamiento de datos almacenen como mínimo seis meses los datos de tráfico o "relativos a las comunicaciones electrónicas". La ley no cuenta con los estándares mínimos para salvaguardar la información privada de los usuarios ni criterios para justificar el almacenamiento de más datos de los que la empresa necesita (Rolón y Sequera, 2016).

Otro ejemplo es la Resolución Nº 1.350/2002[8] de la Comisión Nacional de Telecomunicaciones (Conatel), que en el artículo 26 contradice la Ley Nº 642/95 de Telecomunicaciones. Esta resolución otorga facultades a las compañías operadoras de servicios de telefonía para almacenar por un periodo de seis meses el registro de detalles de llamadas de todos los usuarios en Paraguay. Esta medida preinvestigativa para cualquier tipo de ilícito es desproporcional con relación al fin perseguido. Además, deja de lado el ideal de una intervención mínima a través del aparato punitivo del Estado, propio de lo que se denomina "derecho penal mínimo".

5 Caso Escher y otros vs. Brasil. Sentencia de 6 de julio de 2009 (Excepciones Preliminares, Fondo, Reparaciones y Costas), párr. 114. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf

6 Ibídem.

7 Tedic, 7 de setiembre de 2016. Disponible en: https://www.tedic.org/informeepupy/; Tedic, 2 de noviembre de 2015. Disponible en: https://www.tedic.org/tedic-presenta-el-informe-epu-antes-naciones-unidas/

8 Resolución Nº 1350/02 "Por la cual se establece la obligatoriedad de registro de detalles de llamadas por el plazo de seis meses".

Otro caso emblemático de proyectos legislativos que ponen en peligro la vigencia del derecho a la privacidad es el de "Pyrawebs", como se denominó popularmente al proyecto de ley de retención de datos de tráfico. El proyecto tenía por objetivo obligar a las operadoras a retener los metadatos de las comunicaciones de todas las personas –inocentes o no de algún delito– por doce meses bajo la excusa de la lucha contra el narcotráfico, el terrorismo y la pornografía infantil. No prosperó gracias a la presión de la ciudadanía, que se manifestó en contra de este proyecto.

Sin embargo, en coyunturas marcadas por la violencia, hechos delictivos o inestabilidad política, el Estado paraguayo ha logrado promover leyes de excepción como la ley contra el "terrorismo"[9] o leyes de emergencia penal como el proyecto de ley "contra el crimen organizado[10]". En el marco de estos o con el espíritu que subyace a estas iniciativas, ha adquirido software de vigilancia sin control ni regulación alguna.

Vigilancia 2.0: el Estado se arma para la era digital

Hoy en día, existen tecnologías que facilitan la vigilancia estatal de forma fácil, eficiente y de bajo costo. El Estado paraguayo ha obtenido una serie de herramientas que sirven a este propósito. Por ejemplo, hay evidencias que dan cuenta de la compra del software *Finfisher*[11], un malware de vigilancia altamente invasivo desarrollado por la empresa norteamericana Gamma. Fue adquirido por la Secretaría Nacional Antidrogas (Senad)[12], según consta en publicaciones de facturas y recibos de compra del periódico ABC Color e investigaciones del Citizen Lab de la Universidad de Toronto de Canadá.

Finfisher permite a las autoridades seguir los movimientos de cada persona usuaria de celular u otro dispositivo seleccionado. Específicamente, da la posibilidad de navegar por el historial de las ubicaciones de una persona por años; grabar, encubiertamente, audio y video de micrófonos y cámaras del teléfono inteligente y laptop del objetivo; recuperar la lista de contactos o remotamente implantar evidencia incriminatoria en el dispositivo de la persona usuaria.

También existen registros de adquisición de software de escuchas telefónicas por parte del Estado. Wikileaks ha filtrado conversaciones diplomáticas entre

9 Ley Nº 4024/10 "Que castiga los hechos punibles de Terrorismo, Asociación Terrorista y Financiamiento del Terrorismo".

10 Proyecto de ley presentado por los senadores Fernando Silva Facetti, Enrique Bacchetta y Roberto Acevedo el 2 de octubre de 2013.

11 Tedic, 20 de mayo de 2016. Disponible en: https://www.tedic.org/mas-preguntas-y-dudas-sobre-software-malicioso-adquirido-por-senad/; Citizen Lab, 15 de octubre de 2015. Disponible en: https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/

12 ABC Color, 30 de junio de 2013. Disponible en: http://www.abc.com.py/edicion-impresa/judiciales-y-policiales/senad-gasto-casi-g-200-millones-solo-en-montaje-y-configuracion-590062.html?fb_comment_id=419236824858112_2094744#f1c83727667f9fc; Hoy, 28 de junio de 2013. Disponible en: http://www.hoy.com.py/nacionales/senad-niega-negociado-en-compra-de-equipo-de-escuchas

el Ministerio del Interior y la Embajada de los Estados Unidos del año 2010 en las que se habla de la compra de un software de escuchas telefónicas[13]. Otro caso similar ocurrió durante el gobierno de Federico Franco, que adquirió también un equipo de escuchas telefónicas por valor de 2,5 millones de dólares. Misteriosamente, el equipo desapareció de las oficinas del Ministerio del Interior, según un informe de la Auditoría General del Poder Ejecutivo de noviembre de 2013. Con estos antecedentes, se realizan escuchas telefónicas sin orden judicial[14], bajo la excusa de que se utilizarán única y exclusivamente para los casos de extorsión y secuestro, según el representante del Ministerio del Interior comisario Francisco Alvarenga, violentando de este modo el debido proceso.

Finalmente, Wikileaks, a través de una filtración de uno de los proveedores de malware más notorios del mundo –la empresa italiana *Hacking Team*– y el cuidadoso trabajo de periodistas de investigación, revelaron que el Ministerio Público, a través de la Fiscalía de Delitos Informáticos, ha mantenido conversaciones para la compra de un software de vigilancia[15]. No se corroboró aún que la compra se haya realizado hasta el presente.

La vigilancia en la práctica: el caso de espionaje de las Fuerzas Militares a una periodista

Al Estado paraguayo se le ha acusado de casos concretos y graves de vigilancia ilegal, que violan no solo el derecho a la privacidad, sino también la libertad de expresión y de prensa. El espionaje de las Fuerzas Militares a una periodista de ABC Color es uno de estos casos[16]. Según las denuncias, el sistema de inteligencia conformado para las operaciones del gobierno en el Norte del país contra el grupo criminal Ejército del Pueblo Paraguayo (EPP) fue utilizado para acceder a las comunicaciones de una periodista que realizaba investigaciones sobre corrupción en la cúpula castrense. La Fiscalía tomó nota de este caso y confirmó las acusaciones, afirmando que prepararía una imputación[17].

Este caso comprueba las reiteradas denuncias y reclamos sobre la forma en que el Estado puede vulnerar las comunicaciones privadas de las personas. Además, pone de relieve el rol del sector privado, específicamente el de empresas de telefonía y proveedoras de internet como Personal en este caso, en las actividades de espionaje estatal[18]. Son empresas que acumulan grandes cantidades de datos

13 Wikileaks, 18 de febrero de 2010. Disponible en: https://wikileaks.org/plusd/cables/10ASUNCION97_a.html

14 Telefuturo, 26 de noviembre de 2014. Disponible en: https://www.youtube.com/watch?v=3Bkdspxhae8

15 Wikileaks, 8 de julio de 2015. Disponible en: https://wikileaks.org/hackingteam/emails/emailid/249535

16 ABC Color, 26 de agosto de 2016. Disponible en: http://www.abc.com.py/edicion-impresa/notas/gobierno-uso-su-sistema-de-inteligencia-para-espiar-periodista-1511976.html

17 ABC Color, 31 de agosto de 2016. Disponible en http://www.abc.com.py/edicion-impresa/politica/la-fiscalia-prepara-imputacion-por-violacion-del-secreto-de-comunicacion-1513910.html

18 Tedic, 5 de setiembre de 2016. Disponible en: https://www.tedic.org/personal-debe-posicionarse-publicamente-en-contra-de-la-vigilancia-estatal-ilegal/

de las comunicaciones privadas de millones de paraguayos y paraguayas. Su colaboración o complicidad es clave para que las instituciones públicas puedan monitorear con efectividad las comunicaciones de las personas.

Libertad de expresión en internet

El caso más notorio de avance contra la libertad de expresión en internet ha sido la aprobación de la Ley Nº 5653/16 "De protección de los niños, niñas y adolescentes contra contenidos nocivos en internet" (Tedic, 2016b). Esta ley busca regular las redes de acceso público a internet, como plazas, cibercafés y restaurantes, obligando a responsables de estos lugares y a proveedores del servicio a instalar filtros de bloqueo de "contenidos nocivos" para niñas, niños y adolescentes. Además de los problemas técnicos y de aplicación efectiva que presenta la ley, la misma puede convertirse en una herramienta de bloqueo y censura en internet, violando el derecho al acceso a información y la libertad de expresión.

Si bien la ley persigue un objetivo legítimo, que es la protección de los niños, niñas y adolescentes ante contenidos que pueden afectar su desarrollo, tiene varias limitaciones. Una de estas es que no cumple con el principio de legalidad porque no define qué vuelve "nocivo" a un contenido. Esta falta de precisión impide que las personas conozcan los alcances de la ley y puedan prever su aplicación. Abre también la posibilidad de censura a contenidos legítimos.

Otra limitación grave de la ley, que puede dar pie a la violación de la libertad de expresión, es la creación de listas de bloqueo en internet a través de un órgano administrativo. Según la ley, un Observatorio para la protección de los Derechos del Niño, Niña y Adolescentes en Paraguay tendrá a su cargo la identificación de contenidos y sitios que se consideren nocivos. A partir de este trabajo, se generarán listas de los sitios y contenidos a ser bloqueados de forma compulsiva, vinculante y con sanciones a las empresas proveedoras de internet que no cumplan con la medida. Es problemático que instituciones administrativas, que no están capacitadas para tomar decisiones judiciales sobre la legalidad de la censura de las comunicaciones, las tecnologías utilizadas y los derechos humanos, tengan esta responsabilidad. Existe el riesgo de que, bajo la apariencia de un reclamo administrativo, se restrinja contenido constitucionalmente válido.

Libre acceso a la información en internet

Paraguay cuenta con garantías para cumplir con el derecho de las personas a acceder a información. Pero así como ha habido importantes avances en esta área, también existen desafíos para satisfacer este derecho acorde al avance de las nuevas tecnologías. La Constitución Nacional lo reconoce en el artículo

28 del "Derecho a Informarse". A partir del 2014, el país cuenta con la Ley Nº 5282/14 "De libre acceso ciudadano a la información pública y transparencia gubernamental", una herramienta legal fundamental para que las personas puedan monitorear el desempeño de las autoridades y ejercer otros derechos. Entre otras cosas, el reglamento de la ley dispone la creación de un portal en internet donde se pueden hacer las solicitudes de información pública[19], lo que facilita a la ciudadanía realizar sus peticiones. También, desde el año 2012, Paraguay forma parte de la Alianza de Gobierno Abierto, una iniciativa mundial que promueve la transparencia, la rendición de cuentas y la participación ciudadana, usando la tecnología de forma transversal. A través de esta iniciativa, se han presentado tres planes de acción con compromisos del Gobierno paraguayo que buscan fortalecer el acceso de las personas a información pública y a servicios estatales a través de internet, con la creación de portales de datos abiertos, aplicaciones web, entre otros[20].

Los desafíos pendientes son varios. Primeramente, Paraguay sigue siendo un país que se caracteriza por la desigualdad en el acceso a internet. Según Conatel, a junio de 2016 había más de 3 millones de personas conectadas (Conatel, 2016). Esta brecha digital deja a amplios sectores de la población sin las oportunidades que brinda la red. Además, no todas las instituciones del Estado, municipios y gobernaciones adhieren plenamente a lo establecido en el reglamento de la Ley Nº 5282/14. Algunas no se encuentran en el Portal de acceso a información pública[21], o no responden en tiempo y forma los pedidos de la ciudadanía[22]. Además, investigadores, investigadoras y personas usuarias de datos gubernamentales han citado problemas de accesibilidad, usabilidad y reutilización de la información pública en internet, una suerte de "techo de vidrio" que impide el pleno ejercicio del derecho al acceso a información[23]. Entre otras cosas, se han registrado las siguientes limitaciones: formatos cerrados de publicación que dificultan la reutilización de la información; acceso denegado a información por cuestiones políticas, cambio de autoridades o miedo del funcionariado público; registro incompleto o irregular de datos gubernamentales (Acuña y Masi, 2016).

19 Portal de solicitudes de información pública. Disponible en: http://informacionpublica.paraguay.gov.py/portal

20 Gobierno Abierto Paraguay. Disponible en: http://www.gobiernoabierto.gov.py/

21 82 instituciones suscriben al Portal de acceso a información pública.

22 Vanguardia, 30 de julio de 2016. Disponible en: http://www.vanguardia.com.py/2016/07/30/instan-a-demanda-masiva-por-la-falta-de-acceso-a-la-informacion/; ABC Color, 7 de octubre de 2016. Disponible en: http://www.abc.com.py/edicion-impresa/judiciales-y-policiales/urgen-cumplimiento-de-fallo-que-ordena-proveer-informacion-publica-1525626.html

23 Tedic, 18 de agosto de 2016. https://www.tedic.org/congreso-limita-uso-de-datos-oficiales-para-la-creacion-de-nuevas-herramientas-ciudadanas/

Neutralidad en la Red, un principio clave para el cumplimiento de derechos

La neutralidad en la red es un principio que estipula que los proveedores de servicios de internet deben tratar a todo el tráfico por igual, sin discriminarlo o sin dar preferencia a ciertos contenidos por encima de otros. Este es un principio clave para garantizar los derechos al acceso a información y la libertad de expresión en la red. Por un lado, su incumplimiento deriva en que las personas sean inducidas a acceder a algunos tipos de información y, por otro, la discriminación de contenidos puede ser una forma de censura.

En Paraguay, Conatel debe velar por el cumplimiento de la neutralidad de la red como rector de prácticas comerciales y garante de una internet libre y abierta, para lo cual el control y la supervisión ciudadana son claves[24]. Sin embargo, se han cometido varios abusos en los últimos años sin ningún tipo de sanción. Un ejemplo son las operadoras de internet que privilegian indebidamente algunos contenidos o servicios con aplicaciones gratuitas como Whatsapp o Facebook. También se han registrado bloqueos de páginas web y disminución o discriminación de descarga P2P (Fundación Karisma, 2016).

La ciberseguridad como nuevo campo de acción del Estado

El Estado paraguayo no escapa de la tendencia mundial de entender y hablar sobre los nuevos desafíos que supone internet en términos de "ciberseguridad". Aunque se disputa la definición misma del término, por lo general se entiende por ciberseguridad lo relacionado a la seguridad de la infraestructura crítica de un Estado. En pocas palabras, sus redes y sistemas informáticos que hoy en día son vulnerables a ataques diversos. Pero las discusiones de los Estados en torno al tema se sostienen en conceptos limitados de lo que significa seguridad. Además, se coloca en el centro del diseño de políticas al Estado, dejando de lado a los usuarios de internet y marginando una visión de derechos y desarrollo económico. El primer plan nacional de ciberseguridad de Paraguay refleja este desbalance[25].

Tedic realizó varias críticas y recomendaciones a la propuesta del plan liderado por el Equipo de Respuesta de Incidentes de Seguridad Informática de Paraguay, CERT-Py (Tedic, 2016a), dependiente de la Secretaría Nacional de Tecnologías de la Información y Comunicación (Senatics)[26]. Algunas de estas fueron: la ausencia de nociones de derechos humanos y desarrollo económico en el

24 El artículo 26 de la Resolución Nº 190/09 explicita "la prohibición que tienen los prestadores del servicio de acceso a internet y transmisión de datos de interferir o degradar el tráfico recibido o generado por el usuario o variar la capacidad contratada según el tipo de contenido, aplicación, origen o destino decidido por el usuario".

25 Senatics, 18 de diciembre de 2015. Disponible en: https://www.senatics.gov.py/noticias/exponen-avances-dentro-del-plan-nacional-de-ciberseguridad

26 CERT- Py (s/f). Disponible en: https://www.cert.gov.py/index.php/noticias/finfisher-y-su-relacion-con-paraguay

plan, que deberían ser pilares fundamentales de la seguridad digital o ciberseguridad; hacer de la persona/usuario el centro de esta política pública, más allá de la infraestructura crítica; la falta de políticas de transparencia; la exclusión del plan de actores de internet como la academia, las empresas, organizaciones de la sociedad civil para una cogobernanza efectiva y para hacer contrapeso a la presencia de los sistemas de inteligencia, fuerzas militares y policías.

RECOMENDACIONES

- Impulsar una legislación de protección de datos que contemple una autoridad competente para investigar violaciones de principios de protección de datos personales y ordenar reparación de daños.

- Cumplir los compromisos asumidos en los instrumentos internacionales de carácter vinculante, las recomendaciones y observaciones de las Naciones Unidas mencionadas en el Examen Periódico Universal ante el Consejo de Derechos Humanos del año 2016.

- Proporcionar a la ciudadanía información suficiente sobre el alcance y la naturaleza de la utilización de los software de vigilancia en su poder.

- Modificar el artículo 10 de la Ley de Comercio Electrónico en lo que hace a la retención de datos de comunicaciones en internet para fines comerciales y la resolución de Conatel sobre almacenamiento de datos de llamadas telefónicas por violar el derecho a la privacidad.

- Establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas sobre sus actividades de vigilancia y censura de las comunicaciones.

- Aplicar sanciones a las proveedoras que tienen la gestión y el control de tráfico de datos de las comunicaciones que violen la neutralidad en la red.

- Definir una política pública robusta para proveer de acceso a internet a toda la población, acompañada de programas de capacitación y entrenamiento para su uso responsable.

- Mejorar el acceso a la información pública con base en las necesidades de las personas (la demanda de información), con estándares de datos abiertos y con especial atención a las personas que generan conocimientos a partir de la información pública, puesto que estos pueden contribuir al diseño de mejores políticas públicas del Estado.

BIBLIOGRAFÍA

Acuña, Jazmín y Fernando Masi (2016) *Usos de la información pública para la producción de conocimientos en Paraguay. Hallazgos preliminares*. Asunción: Cadep/CONACYT.

Comisión Nacional de Telecomunicaciones (2016) *Suscripciones de internet por tipo de tecnología de acceso. Informe semestral 2016*. Asunción: Conatel. Disponible en: https://www.tedic.org/wp-content/uploads/sites/4/2016/11/1141261-PLANILLA_20-septiembre-2016_1038_1PDF-PLANILLA_20-septiembre-2016_1038_1.pdf

Ferrajoli, Luigi (1995) "Derecho Penal Mínimo y Bienes Jurídicos Fundamentales" en VV.AA. *Prevención y Teoría de la Pena.* Santiago: Editorial Jurídica Conosur.

Fundación Karisma (2016) *Cómo se contrata en América Latina el acceso a internet.* Disponible en: https://www.tedic.org/wp-content/uploads/sites/4/2016/06/Informe-ISOC-Final-jun-27.pdf

Rolón, Jorge y Maricarmen Sequera (2016) *Vigilancia estatal de las comunicaciones y derechos fundamentales en Paraguay.* Disponible en: https://www.tedic.org/wp-content/uploads/sites/4/2016/05/Paraguay-ES.pdf

Tedic (2016a) Comentarios al borrador del plan de ciberseguridad. Disponible en: https://www.tedic.org/wp-content/uploads/sites/4/2016/06/observaciones-sobre-el-plan-de-ciberseguridad_v14jun-.pdf

Tedic (2016b) *Análisis jurídico sobre el proyecto de ley de contenidos nocivos en internet para niños y adolescentes.* Disponible en https://www.tedic.org/tedic-no-esta-de-acuerdo-con-el-enfoque-de-tecnologia-que-tiene-el-proyecto-de-proteccion-de-la-ninez-de-contenidos-nocivos-en-internet/

United Nations (2014) *The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights.* Disponible en: https://eff.org/r.hz9z