

Asunción 4 de diciembre de 2017

Sr. David Kaye
Relatora Especial de las Naciones Unidas sobre la libertad de expresión y opinión
OHCHR - Palais Wilson
52, rue des Pâquis
CH-1201 Ginebra
Suiza

Re: Contribuciones escritas para la presentación sobre libertad de expresión en la era digital en Paraguay

Distinguido relator,

TEDIC¹ es una organización sin fines de lucro con sede en Asunción, Paraguay, que defiende los derechos humanos en Internet. Respetuosamente enviamos esta carta a la Relatoría Especial de las Naciones Unidas sobre la libertad de expresión en la era digital: “**Submission to study on social media, search, and freedom of expression**” para la consideración de su informe anual que será publicado en el 2018.

Marco Legal

La Constitución de la República del Paraguay, en su artículo 26 (Libertad de expresión y prensa) establece que

“Se garantizan la libre expresión y la libertad de prensa, así como la difusión del pensamiento y de la opinión, sin censura alguna, sin más limitaciones que las dispuestas en esta Constitución; en consecuencia, no se dictará ninguna ley que las imposibilite o las restrinja. No habrá delitos de prensa, sino delitos comunes cometidos por medio de la prensa”.

Esta disposición constitucional se aplica a la expresión en cualquiera de sus formas, incluida la que se difunde a través de Internet.

En Paraguay, los tratados internacionales ratificados por el Congreso gozan de una jerarquía normativa inferior a la de la Constitución, pero superior a la de las leyes (Art. 137). En particular, se aplican las disposiciones sobre *libertad de expresión* contenida en los siguientes tratados internacionales de los que el Paraguay es parte: Artículo 13 de la Convención Americana de Derechos Humanos, Declaración Universal de Derechos Humanos (Arts. 19 y 29), Pacto Internacional de Derechos Civiles y Políticos (Arts. 19 y 20), Convención sobre los Derechos del Niño (Art. 13), Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial (Art. 4).

¹ **Asociación TEDIC:** Organización sin fines de lucro con sede en Asunción, Paraguay que desarrolla tecnología cívica y defiende los derechos humanos en Internet. Mas información en www.tedic.org

Por otro lado, cabe recordar que el Código Penal (Ley 1160/97) tipifica los hechos punibles de *calumnia, difamación e injuria* en los artículos 150, 151 y 152 respectivamente, que son una limitación a la *libertad de expresión* y que se aplican sin que se distinga el medio a través del cual se los comete, por lo que obviamente incluye a Internet.

Un proyecto de ley de censura política

El proyecto de ley “Que obliga a proveedores de aplicaciones y redes sociales a suspender y retirar publicaciones con carácter ofensivo o difamatorio”² presentado por el Diputado Nacional Edgar Ortiz, se suma a la lista de iniciativas legislativas que buscan regular Internet e forma regresiva. Con esto se termina coartando las libertades que este espacio posibilita: la libertad de las personas de informarse, de expresar sus opiniones y de debatir, todas acciones propias de una sociedad democrática. El proyecto de ley, además de contener problemas de forma y de ser esencialmente inviable en la práctica, es redundante, desproporcional y violatorio de derechos fundamentales protegidos por la Constitución, como por ejemplo, el derecho a la libertad de expresión y el debido proceso³.

Sumado a lo anterior, la propuesta genera redundancia legislativa, en vista a que los hechos punibles contra el honor y la reputación ya se encuentran regulados en el Código Penal paraguayo: calumnia, difamación e injuria como ya se comentó anteriormente.

Las expresiones ofensivas, falsas u odiosas no pueden quedar impunes, pero creemos que existen mecanismos legales para perseguir hechos punibles, siempre y cuando medie una orden judicial. Además es inadmisibles que aquellos que hacen política partidaria y actúan en la esfera pública, pretendan suprimir el legítimo disenso y el diálogo, usando esta herramienta para escapar a las críticas y a la auditoría social, ambas garantías constitucionalmente establecidas. La propuesta legislativa exige identificación y bloqueos que conforman una grave amenaza al ejercicio de la ciudadanía. Una medida desproporcionada e innecesaria para la protección del honor y la reputación en el entorno en línea.

Otro elemento a considerar es que el proyecto carece garantías mínimas para justificar cualquier censura e impone una medida desproporcionada –la remoción de contenidos de Internet– sin contemplar el debido proceso. Por ejemplo, no hace mención a la necesidad de contar con una orden judicial para remover dichos contenidos, en el marco de un proceso legal. Esto obligaría a los intermediarios de Internet (OTT) a eliminar comentarios, contenidos o perfiles, volviendo este procedimiento altamente peligroso ya que “abre las puertas” para ejercer un control indiscriminado de los contenidos en Internet.

La Relatoría Especial de Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) analizó este tema y realizó propuestas relativos a los intermediarios, en el Capítulo IV del informe 2013⁴. Se advierte sobre los posibles peligros y/o abusos que los administradores de red, así como aplicaciones de contenidos pueden ejercer en Internet.

2 Proyecto de ley “Que obliga a proveedores de aplicaciones y redes sociales a suspender y retirar publicaciones con carácter ofensivos o difamatorio” <http://sil2py.senado.gov.py/formulario/FichaTecnicaExpediente.pmf?q=FichaTecnicaExpediente%2F110839> [Fecha de consulta: 20 de octubre, 2017].

3 Análisis y posicionamiento de la ONG TEDIC <https://www.tedic.org/un-proyecto-de-censura-politica/> [Fecha de consulta: 20 de noviembre, 2017].

Por su parte, la Relatoría especial de Naciones Unidas (ONU) para la libertad de expresión, en su informe⁵ sobre la *promoción y protección del derecho a la libertad de expresión en Internet*, elaboró una serie de requisitos que establecen que las restricciones de contenidos en Internet sólo se podrán realizar como excepcionales, siempre y cuando se cumplan los siguientes criterios: *el principio de legalidad*, es decir que esté prevista en la ley, que debe ser clara y accesible por todos; que hayan *agotado todas las instancias* ordinarias para alcanzar el objetivo; que la medida sea *proporcional y necesaria*; y que la misma persiga uno de los objetivos establecidos en el artículo 19, párrafo 3 del Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por su sigla en inglés).

Otra preocupación que surge con este proyecto de ley, es la subjetividad de la denuncia sin análisis de los contenidos por algún órgano judicial independiente. Esto provoca que la definición de lo que *puede ser considerado ofensivo* queda al arbitrio de cualquier “partido, movimiento o candidato” y sumado a la dificultad de establecer de “*qué es falso*” permiten que cualquier postura sea potencialmente denunciada como irregular. Es decir, que por simple solicitud por parte de los políticos, el contenido debe removerse o suspenderse: esta censura previa por uno o varios órgano/s administrativo/s sin el debido proceso violenta las garantías consagradas en nuestra Constitución.

Se debe tener en cuenta que los intermediarios de Internet no están “capacitados” en lo referente al debido proceso: por tanto no son competentes para tomar decisiones judiciales sobre la legalidad de la censura de las comunicaciones, las tecnologías utilizadas y los derechos humanos. Este “procedimiento” que aparece como una “solicitud administrativa” a las aplicaciones de contenidos, que depende de una interpretación subjetiva de actores políticos, abre la posibilidad de censura de cualquier contenido.

La propuesta legislativa sanciona el anonimato

Desde la perspectiva del proyecto, las aplicaciones de contenido y redes sociales tendrían que proporcionar el nombre completo, la identificación y “*el número de seguridad social*” del titular del perfil, para que el contenido pueda permanecer *en-línea* (Art 1). Lo que no queda claro es a quién debería remitirse dicha información, así como tampoco se establecen los tiempos de censura de los contenidos en cuestión.

El legislador no tiene en cuenta que el *principio del anonimato* es una forma de libertad de expresión. David Kaye, relator especial para la libertad de expresión de ONU, en su informe⁶ sobre la importancia del cifrado y anonimato para libertad de expresión, manifestó lo siguiente: “*la encriptación y el anonimato proporcionan la privacidad y la seguridad necesarias para el ejercicio de la libertad de opinión y de expresión en la era digital*”. Siguiendo esa premisa, el relator recomienda entre otras cosas que “*las legislaciones nacionales deben reconocer que los individuos son libres de proteger la privacidad de sus comunicaciones digitales mediante el*

4 Informe La Relatoría Especial de Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) <https://www.oas.org/es/cidh/expresion/temas/internet.asp> Fecha de consulta: 20 de octubre, 2017].

5 Relatoría Especial de Libertad de expresión en la era digital. ONU <http://www.ohchr.org/SP/Issues/FreedomOpinion/Pages/OpinionIndex.aspx>.

6 Cifrado y anonimato para la libertad de expresión <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx> [Fecha de consulta: 20 de octubre, 2017].

uso de tecnologías de cifrado y herramientas que permiten el anonimato en línea”. Además, destaca que se debe promover el acceso y el uso a estas herramientas y tecnologías. Según Kaye, los debates sobre cifrado y anonimato han sido polarizados en el discurso por su uso potencialmente criminal.

Por tanto, se sugiere que el debate debería cambiar para destacar la protección que ofrecen este tipo de herramientas a los individuos, especialmente a los grupos que viven en situaciones de riesgo: periodistas, defensores de derechos humanos, activistas, entre otros.

Libre acceso a Internet

Según CONATEL⁷, a junio de 2016 habían más de 3 millones de personas conectadas⁸ a Internet. Por otra parte, según las publicaciones de la Secretaría Nacional de Tecnología de la Información y Comunicación (SENATICs)⁹, actualmente el 90% de población accede a Internet a través de telefonía móvil. A partir de estas constataciones surgen varios desafíos. En primer lugar, Paraguay sigue siendo un país caracterizado por la desigualdad en el acceso a Internet: aunque la conexión es masiva, no es de calidad. Los costos de los paquetes de datos son altos, la conexión es lenta y el aumento de cobertura está dado por las ofertas de *zero rating*, que violentan la *neutralidad en la red*.

Esta *brecha digital* deja a sectores de la población sin las oportunidades que brinda la red incluyendo ausencia de políticas con perspectiva de género. En la investigación “*Mejor educar que prohibir*” se expone la diferencia en el acceso a Internet por parte de niños, niñas y adolescentes: las mujeres acceden a un teléfono propio recién a partir de los 14 años, mientras los hombres ya cuentan con su dispositivo desde los 10 años. Esta inclusión tardía, además de otras brechas de desigualdad, generan serios problemas, en un contexto de mayor violencia y desprotección de las niñas y adolescentes, limitando su derecho de libertad de expresión y acceso al conocimiento a través de Internet. Por tanto, se deberán desarrollar planes de inclusión con acompañamiento y protección para ellas.

Neutralidad en la Red

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”, es decir sin discriminar o sin dar preferencia a cierto contenido por encima de otro. 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 termina favoreciendo a los actores más poderosos y limitando la variedad amplitud de contenidos a los que acceden las personas. Por otro, la discriminación de contenidos puede ser una forma de censura y de limitación de la innovación, en tanto dificulta la entrada de nuevos actores al sistema.

En Paraguay, CONATEL, ente regulador de las telecomunicaciones, debe velar por el cumplimiento de la *neutralidad de la red*, como rector de prácticas comerciales y garante de una Internet libre y abierta¹⁰. La actual regulación no se encuentra ampliada en un reglamento u otro instrumento legal distinto de la resolución, que regule este principio. Sin

7 Comisión Nacional de Telecomunicaciones -CONATEL- es el ente regulador de las comunicaciones en Paraguay

8 Suscripciones de Internet por tipo de tecnología de acceso. Informe semestral 2016. CONATEL. [Fecha de consulta: 23 de octubre, 2017].

9 SENATICs [Fecha de de consulta] 27 de noviembre, 2017
<http://gestordocumental.senatic.gov.py/share/s/ntjnuNLeT8u3gbAHC6WeVw>

embargo, en los últimos años, se han cometido varios abusos sin ningún tipo de sanción: un ejemplo de esto son algunas operadoras de Internet que privilegian indebidamente algunos contenidos o servicios con aplicaciones gratuitas como Whatsapp, Facebook u otros atentando justamente con este principio. También se han registrado bloqueos de página web o disminución o discriminación de descarga P2P por parte de operadoras del interior del país¹¹.

El caso de la censura corporativa –Tigo y Personal– que ha bloqueado acceso a una web de parodia del periódico ABC Color también fue una violación de la *neutralidad de la red*. Este tipo de censuras por parte del sector privado pueden ser tan perjudicial como la estatal y en algunos casos más poderosa. Ante esta situación tampoco hubo pronunciamiento ni sanción por parte de CONATEL. Lo interesante del caso, fue la reacción de varios sectores de la ciudadanía que alzó su voz ante este caso de censura, lo que provocó que luego de pocas horas el inconveniente fuera resuelto¹².

Riesgo del derecho a la aparición e identidad

Ser una mujer transexual en Internet aumenta los riesgos de exposición de violencia y otros abusos: expresiones de odio y el cyber-acoso son algunos elementos con los que suelen tener que lidiar aquellas personas cuyas identidades ponen en entredicho la norma social. En muchos casos, la discriminación se inicia con las reglas que imponen las proveedoras de servicio o intermediarios y que no suelen contemplar las múltiples identidades humanas

Las defensoras de los derechos de las mujeres trans en Paraguay, aglutinadas en el colectivo Panambi¹³, se enfrentan constantemente al bloqueo de sus perfiles en redes sociales tales como Facebook. Por lo general, sus cuentas son canceladas luego de ser denunciadas como “perfiles falsos”¹⁴. El problema se agrava cuando solicitan la restitución de sus cuentas y las empresas les exigen documentos legales, como por ejemplo pasaporte o cédula de identidad con su “nombre real”. Es sabido que en Paraguay, el Estado no reconoce legalmente la identidad de las mujeres transexuales por lo que terminan marginadas y de ciertas redes sociales, viendo coartados su derecho a la libre expresión, a la aparición en Internet y a la identidad.

Ausencia de políticas de transparencia sobre “baja de contenidos”

En la investigación “*Quién defiende tus datos*”¹⁵ realizada por TEDIC, se han evaluado a las proveedoras de Internet más importantes del país, en lo que respecta a sus políticas y prácticas de protección de derechos humanos en Internet. Uno de los hallazgos más

10 Artículo 26 de la Resolución No. 190 de 2009 “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”

11 Ver informe de Neutralidad en la Red Paraguay y Latinoamérica. Disponible en <https://www.tedic.org/wp-content/uploads/sites/4/2016/06/Informe-ISOC-Final-jun-27.pdf> [Fecha de consulta: 23 de noviembre, 2017].

12 Por detalles del caso, acceder a “Roben este post” disponible en <https://medium.com/@TEDICpy/roben-este-post-neutralidad-en-la-red-9a3567cd7fb0> [Fecha de consulta: 23 de noviembre, 2017].

13 Mas información <http://www.panambi.org.py/> [Fecha de consulta: 23 de noviembre, 2017].

14 El derecho a aparición en Internet de la comunidad LGBTIQ. TEDIC, 5 de junio de 2017. <https://www.tedic.org/el-derecho-a-aparicion-en-internet-de-la-comunidad-lgbtig/> [Fecha de de consulta: 27 de noviembre, 2017]

15 Investigación “Quién defiende tus datos” Abril 2017. <https://qtdt.tedic.org/> [Fecha de de consulta] 27 de noviembre, 2017

preocupantes es que las ISP locales no cumplen con los estándares de transparencia, según el Principio 21 de los “Principios Rectores sobre las Empresas y los Derechos Humanos” de la Organización de Naciones Unidas.

En dicha investigación, también se evaluaron políticas de *bloqueos, filtrado o retiro de contenidos* en Internet y ver si estos procedimientos revisten de carácter judicial. Lo que se encontró es que ninguna de las ISP evaluadas cumplen con este criterio. En particular, se pudo constatar que una de las proveedoras evaluadas filtra las descargas que utilizan tecnologías peer-to-peer (P2P).

Aunque las ISP no han adoptado medidas contractuales para el bloqueo de acceso a Internet, existen evidencias que sí han hecho acuerdos como se evidencia en el caso del bloqueo de una página web de parodia sobre el periódico ABC Color en el año 2010¹⁶. Afortunadamente no han habido evidencias de nuevos bloqueos similares.

Libertad de expresión en riesgo: “contenidos nocivos”

El caso más notorio de atentado contra la libertad de expresión en Internet ha sido la aprobación de la Ley “De protección de los niños, niñas y adolescentes contra contenidos nocivos en Internet”¹⁷ ¹⁸. Esta Ley busca regular el acceso a Internet en las redes de acceso público disponibles en plazas, cibercafés, restaurantes y otros, obligando a los responsables de estos espacios, así como a los proveedores del servicio, a instalar filtros de bloqueo de “contenidos nocivos” para los 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 de acceso a la información y la libertad de expresión.

Si bien la Ley persigue un objetivo legítimo, que es el de proteger a los niños y niñas de contenidos que pueden afectar su desarrollo, tiene varias limitaciones: una de éstas es que no cumple con el principio de legalidad, porque no define los criterios bajo los cuales considerar “nocivo” a ciertos contenidos. Esta falta de precisión impide que las personas conozcan los alcances de la Ley y puedan prever su aplicación, del mismo modo que abre la posibilidad de censura ilegítima de contenidos.

Otra limitación de la Ley, que puede dar pie a la violación de la libertad de expresión, es la creación de listas de bloqueo en Internet que se construirán a través de un órgano administrativo. Según la Ley, se creará un “Observatorio para la protección de los Derechos del Niño, Niña y Adolescentes en Paraguay” que 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

16 Paraguayan ISP Censoring site for mocking stockholder's paper - The Largest in the Country. <https://www.tedic.org/paraguayan-isp-censoring-site-for-mocking-stockholders-paper-the-largest-in-the-country/> [Fecha de consulta: 27 de noviembre, 2017]

17 Ley “De protección de los niños, niñas y adolescentes contra contenidos nocivos en Internet” <http://www.bacn.gov.py/leyes-paraguayas/5167/proteccion-de-ninos-ninas-y-adolescentes-contra-contenidos-nocivos-de-internet>

18 Ver análisis jurídico y técnico de TEDIC. 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/> [Fecha de consulta: 20 de octubre, 2017].

a las empresas proveedoras de Internet que no cumplan con la medida. Resulta problemático el hecho de 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. Debido a esto aparecen los riesgos de filtrar contenidos que sean legítimos bajo la apariencia de un reclamo administrativo.

Educación con perspectiva de género en retroceso

Una de las acciones más alarmantes y regresivas en materia de derechos del gobierno del presidente Horacio Cartes, ha sido una resolución del ministro de educación Enrique Riera que prohíbe la utilización y difusión de materiales didácticos digitales o impresos que hagan referencia a la “ideología de género” o “teoría de género”¹⁹. La resolución 29664 ha sido el resultado del lobby de grupos religiosos conservadores que buscan revertir los avances en materia de derechos que se han conseguido con el esfuerzo de millones de mujeres y activistas LGBTI de todo el mundo. La prohibición viola el derecho al acceso a la información de la ciudadanía, amparado en el artículo 28 de la Constitución Nacional, el derecho a la identidad y a la libertad de expresión. Esta prohibición o censura atenta contra la declaración de los derechos del niño que Paraguay firmó como Estado miembro de ONU. La abogada y feminista Line Bareiro considera que con esta resolución ministerial se anula la posibilidad de entender cómo se construyen las relaciones de poder en la sociedad. Lo plantea de la siguiente forma: *“Al prohibir la teoría de género Riera prohibió que se hable de [...] lo público y lo privado y lo productivo y reproductivo. Lo público construido como masculino y lo privado, familiar como femenino”*.

Esta prohibición ignora que en Paraguay, hay 6 niñas y adolescentes que son abusadas sexualmente por día²⁰; o que existen unas 20 mil embarazadas por año, de las cuales 684 son niñas de entre 10 y 14 años²¹; o que cada 9 días ocurre un feminicidio²². No hay forma de hacer frente a estos problemas sin que se promueva la educación con perspectiva de género en escuelas y colegios. Solo una sistema educativo que deconstruya el poder del patriarcal será capaz de contrarrestar la violencia de género en todas sus formas: física, sexual, psicológica y económica.

Las barreras y los estereotipos que restringen el desarrollo de todas las personas, por limitarlas a expectativas socialmente construidas, no se pueden superar si no se habla de las creencias y valores que sostienen estos límites. Para esto, hay que incorporar un enfoque de género desde los años de formación.

19 MEC prohíbe uso de materiales sobre “ideología de género”. Última Hora - Octubre 2017. <http://www.ultimahora.com/mec-prohibe-uso-materiales-ideologia-genero-n1112372.html> [Fecha de de consulta: 27 de noviembre, 2017]

20 Cada día, seis niños, niñas y adolescentes son abusados en Paraguay. Ñanduti, Mayo de 2017. <http://www.nanduti.com.py/2017/05/25/cada-dia-seis-ninos-ninas-y-adolescentes-son-abusados-en-paraguay/> [Fecha de de consulta: 27 de noviembre, 2017]

21 Más de 680 niñas con edades de 10 a 14 años dieron a luz el año pasado. ABC Color - Abril de 2015. <http://www.abc.com.py/edicion-impresajudiciales-y-policiales/mas-de-680-ninas-con-edades-de-10-a-14-anos-dieron-a-luz-el-ano-pasado-1361649.html> [Fecha de de consulta: 27 de noviembre, 2017]

22 Cada 9 días una mujer es víctima de feminicidio en Paraguay. Última Hora- Enero de 2017. <http://www.ultimahora.com/cada-9-dias-una-mujer-es-victima-feminicidio-paraguay-n1057722.html> [Fecha de de consulta] 27 de noviembre, 2017

Vigilancia estatal

Hoy en día existen tecnologías que facilitan la vigilancia estatal eficiente y de bajo costo. El Estado paraguayo ha obtenido una serie de herramientas que sirven para este propósito: hay evidencias de la compra del software *Finfisher*²³, un malware de vigilancia altamente invasivo desarrollado por la empresa norteamericana Gamma. El mismo fue adquirido por la Secretaría Anti Drogas (SENAD)²⁴, 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 Canadá²⁵.

Finfisher permite a las autoridades seguir los movimientos de cada usuario de celular u otro dispositivo seleccionado. Específicamente, da la posibilidad de: navegar por el historial de las ubicaciones de un usuario 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 del usuario.

También existen registros de adquisición de software para escuchas telefónicas por parte del Estado: Wikileaks ha filtrado conversaciones diplomáticas entre el Ministerio del Interior y la Embajada de los Estados Unidos del año 2010 donde se habla de la compra de un software de escuchas telefónicas²⁶.

Otro caso similar ocurrió durante el gobierno del ex-presidente Federico Franco, que adquirió también un equipo de escuchas telefónicas por valor de 2,5 millones de dólares. Según un informe de la Auditoría General del Poder Ejecutivo, el equipo desapareció de las oficinas del Ministerio del Interior en noviembre de 2013.

Con estos antecedentes no es de extrañar que se hallan comprobado escuchas telefónicas sin orden judicial²⁷, y que se sigan realizando bajo la excusa de que se utilizan única y exclusivamente para los casos de extorsión y secuestro, violentando así el debido proceso.

Finalmente, a través de una filtración de uno de los proveedores de malware más conocidos del mundo –la empresa italiana *Hacking Team*– usando WikiLeaks, y gracias a un cuidadoso trabajo de periodistas de investigación, se evidenció que el Ministerio Público, a través de la Fiscalía de Delitos Informáticos, ha mantenido conversaciones para la compra de un software de vigilancia de dicha empresa²⁸. No se puede confirmar que la compra se haya realizado hasta ahora.

23 Más preguntas y dudas sobre software malicioso adquirido por SENAD. Disponible en <https://www.tedic.org/mas-preguntas-y-dudas-sobre-software-malicioso-adquirido-por-senad/> y Mapping Finfisher <https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/> [Fecha de consulta: 20 de octubre, 2016].

24 Disponible en Senad gastó casi G. 200 millones solo en “montaje y configuración” 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 y Senad niega la compra del software <http://www.hoy.com.py/nacionales/senad-niega-negociado-en-compra-de-equipo-de-escuchas> [Fecha de consulta: 20 de octubre, 2016].

25 Disponible en <https://citizenlab.org/> [Fecha de consulta: 20 de octubre, 2016].

26 Disponible en https://wikileaks.org/plusd/cables/10ASUNCION97_a.html [Fecha de consulta: 20 de octubre, 2016].

27 Informe Canal 4 Telefuturo: Escuchas telefónicas sin orden judicial se darán en caso de extorsión y secuestro - 26/11/2014 <https://www.youtube.com/watch?v=3Bkdspxae8> [Fecha de consulta: 20 de octubre, 2016].

28 Disponible en <https://wikileaks.org/hackingteam/emails/emailid/249535>

Otra forma de violación de la libertad de expresión se puede apreciar en los casos de espionaje que han afectado a varios países de la región, como Paraguay. En estos casos, fueron monitoreadas de forma ilegal las comunicaciones de mujeres con visibilidad y cierto grado de poder para incidir en políticas, como periodistas y activistas de DDHH.

El espionaje estatal es una violación al derecho a la *libertad de expresión*, la *privacidad* –y cuando afecta a periodistas– al ejercicio de la *libertad de prensa*: todas garantías contempladas en la Constitución de la República.

Más allá, desde una perspectiva de género, la vigilancia se ejerce de tal manera que terminan por controlar, acallar, intimidar o extorsionar a las mujeres que desafían el *statu quo* –el Estado patriarcal. A medida que más mujeres ocupan cargos públicos u oficios donde tradicionalmente los hombres han ejercido protagonismo, la vigilancia emerge como una herramienta para frenar estos avances en equidad. Se convierte en el arma de control de la expresión, el pensamiento y el movimiento de ellas.

El caso más notorio de vigilancia en Paraguay involucró a una periodista del diario ABC Color, el de mayor audiencia del país, que fue espiada por altos mandos militares²⁹ (específicamente un equipo de inteligencia militar con posible apoyo policial). Según denunció el periódico, la vigilancia se realizó en el marco de unas publicaciones sobre corrupción en las Fuerzas Armadas y su objetivo fue conocer quién estaba realizando dicha investigación periodística. Concretamente, fueron interceptados dos celulares para acceder al registro de llamadas, contando con la colaboración de un empleado del servicio de telefonía privada que utilizaba la periodista. A pesar de todas las evidencias recolectadas, hasta hoy en día no han habido significativos avances por parte de la Justicia en este caso.

Por otro lado, el Ministerio Público cuenta con tecnología para intervenir las comunicaciones (incluyendo las comunicaciones a través de Internet) para la persecución de hechos punibles: sistemas de escuchas telefónicas y malwares³⁰. Esta alta tecnología hoy se encuentra cuestionada por menoscabar la garantía del debido proceso por las *Relatorías Especiales de Libertad de Expresión* de ONU y OEA, alegándose que toda violación de la privacidad de cualquier individuo tiene un impacto directo a los sistemas democráticos, así como al derecho a la *libertad de expresión*, ya que la misma genera censura o autocensura.

Por todo lo expuesto hasta el momento, pasamos a listar una serie de sugerencias que podrían tenerse en cuenta a la hora de elaborar recomendaciones

29 Gobierno usó su sistema de inteligencia para espiar periodista <http://www.abc.com.py/edicion-impresa/notas/gobierno-uso-su-sistema-de-inteligencia-para-espiar-periodista-1511976.html> [Fecha de de consulta] 27 de noviembre, 2017

30 Disponible en <https://wikileaks.org/hackingteam/emails/emailid/249535>

Recomendaciones

- Solicitar al Congreso Nacional de Paraguay el *veto del proyecto de ley de censura en Internet*. Dicha propuesta atenta contra la libertad de expresión de la ciudadanía y ataca directamente el derecho a la participación política sin miedo a represalia.
- Transparencia y rendición de cuentas: el Estado paraguayo debe cumplir los compromisos asumidos en el EPU³¹ ante la Organización de las Naciones Unidas. Debe además proporcionar a la ciudadanía información suficiente para que pueda comprender plenamente el alcance y la naturaleza de la utilización de los software de vigilancia en su poder.
- Solicitar al Ministerio de Educación y Cultura la rectificación de la resolución 29664 por violentar derechos fundamentales
- Supervisión pública: el Estado paraguayo debería establecer mecanismos independientes de supervisión para garantizar la transparencia y la rendición de cuentas sobre sus actividades de vigilancia y censura de las comunicaciones.
- Control ciudadano y estatal a las proveedoras de Internet: las proveedoras tienen la gestión y el control del tráfico de datos de las comunicaciones, lo que le otorga el poder de limitar el acceso a contenido en Internet. El control y la supervisión ciudadana y la aplicación de sanciones por parte de CONATEL a violaciones a la neutralidad en la red, son claves para una Internet libre y abierta.
- Investigar las denuncias de espionaje estatal y rendir cuentas sobre las circunstancias en las que se aplica este tipo de medidas: si se aplican principios de respeto a los derechos fundamentales de las personas y el test de proporcionalidad, necesidad e idoneidad.
- Es necesario y urgente elevar los estándares de protección de datos personales para un ejercicio pleno de la *libertad de expresión y privacidad*. En particular, se debe crear una *Ley de Protección de Datos Personales* con un enfoque integral, para evitar los posibles abusos que se realizan con los datos personales tanto en el sector público como el privado.
- Transparencia del sector privado (ISP): el informe de transparencia es un elemento positivo para el resguardo de los derechos humanos. Para un mejor seguimiento de la vigilancia estatal de las comunicaciones, se vuelven elementos clave, el conocer el número global de solicitudes realizadas por las autoridades de persecución penal, las

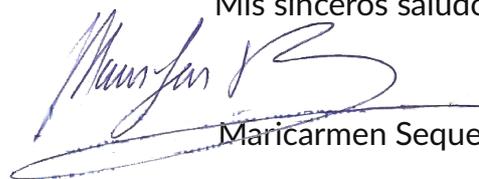
31 En el 2016, el Estado paraguayo se comprometió a cumplir las recomendaciones sobre la privacidad en el Examen Periódico Universal (EPU) para la adopción de medidas necesarias para regular la vigilancia acorde a los principios internacionales de Derechos humanos. Disponible en <https://www.tedic.org/informeepupy/> y TEDIC presenta el informe EPU ante Naciones Unidas <https://www.tedic.org/tedic-presenta-el-informe-epu-antes-naciones-unidas/> [Fecha de consulta: 22 de Noviembre, 2017].

estadísticas respecto a las solicitudes realizadas por otras autoridades, la identificación de las instituciones solicitantes, los tipos de solicitudes y las razones por las que se realizan.

- Profundización de las políticas de cobertura de Internet y de acceso a información: el Estado debe definir una *política pública* robusta para proveer de acceso a Internet a toda la población, acompañado de programas de capacitación y entrenamiento para su uso responsable.
- Diseñar políticas de inclusión efectiva de las niñas, adolescentes y mujeres en el ámbito tecnológico, ya sea a través de programas educativos, talleres de capacitación, provisión de servicios de acceso a Internet de bajo costo o públicos, campañas de concientización sobre los riesgos que existen en la Web y formas de afrontarlos con un enfoque de apropiación, entre otros.
- Garantizar el cumplimiento de los compromisos del Estado, de promoción de igualdad entre hombres y mujeres respetando la legislación y normativas ya existentes.

Gracias por su consideración, cualquier consulta o necesidad de aclaración, no dude en contactarnos.

Mis sinceros saludos,



Maricarmen Sequera

Directora Ejecutiva

TEDIC