EXAMINANDO LOS DERECHOS Y LAS LIBERTADES EN INTERNET EN LATINOAMÉRICA (EXLILA)

INFORME NACIONAL PARAGUAY

Maricarmen Sequera Buzarquis
TEDIC*

RESUMEN EJECUTIVO

Paraguay tuvo una historia de vigilancia estatal y privada durante la dictadura militar de Alfredo Stroessner (1954-1989)[1]. Sin embargo, el período democrático no está exento de prácticas similares o nuevas modalidades de intrusión abusiva en la vida de la ciudadanía.

Este informe analiza la vigilancia y violaciones de los derechos fundamentales que perduran en este período democrático en el Paraguay, en otras modalidades incluyendo la vigilancia a través de internet. Además pone en evidencia la profundización de algunos procesos como endurecimientos de las penas, penalización de nuevas conductas, restricciones al derecho a la defensa, la no vigencia efectiva de las garantías judiciales, la intrusión masiva en la vida privada de las personas y el aumento del poder de los actores principales del sistema penal. Esto se enmarca en una tendencia mundial que se puede denominar "neopunitivismo" para paliar situaciones

* TEDIC – Comunidad y Tecnología es una organización sin fines de lucro que desarrolla tecnología cívica y defiende los derechos humanos en internet en pos de una cultura libre. www.tedic.org

1 https://es.wikipedia.org/wiki/Alfredo_Stroessner

APC
ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES

Este informe se ha elaborado como parte del proyecto Examinando los derechos y las libertades en internet en Latinoamérica (EXLILA) de la Asociación para el Progreso de las Comunicaciones (APC).
El proyecto está financiado por Open Society Institute (OSI) y APC y está coordinado por la ONG Derechos Digitales.

insostenibles[2]. El neopunitivismo a su vez genera cambios normativos que vulneran normas y principios constitucionales y de derecho internacional de derechos humanos, penales y procesales penales.

Paraguay se expande tecnológicamente. Contamos con un 30% de la población que tiene alguna forma conexión a internet. Pero los planes de expansión y conectividad de las empresas privadas no van de la mano con las políticas nacionales de telecomunicación; estas últimas tienen retrasos en regulaciones y aplicación de políticas sobre internet sin perspectiva de derechos humanos.

Por otro lado, existen regulaciones que fortalecen los derechos fundamentales en normas de jerarquía constitucional, ratificaciones de tratados internacionales y regulaciones administrativas sobre derechos humanos que cumplen un papel importante para las bases de un sistema democrático. Paraguay sin duda cumple con los estándares mínimos de defensa de los derechos fundamentales. Pero existen ausencias o fallas en el cumplimiento del debido proceso, notificaciones a las partes y comprensión de que las mismas limitaciones para la intromisión a la intimidad de las personas deberán ser tomadas cuando se trasladan a internet. Hoy, al igual que en la región, la ciudadanía corre un alto riesgo de que se violen sus derechos a la libertad de expresión en internet y la privacidad, debilitando así nuestro sistema democrático.

2 Por ejemplo la guerrilla en Paraguay. Ejército del Pueblo Paraguayo (EPP). https://es.wikipedia.org/wiki/Ej%C3%A9rcito_del_Pueblo_Paraguayo

INTRODUCCIÓN

Los derechos a la intimidad, a la libertad de expresión y al acceso a la información y al conocimiento son derechos esenciales para la dignidad humana y para la prevalencia de una sociedad democrática. No obstante, estos derechos se encuentran amenazados por actores públicos y privados que buscan aprovechar las posibilidades de interferencia en la vida privada de las personas, bloqueo y censura a través de avances tecnológicos.

En la actualidad, el internet de alta velocidad llega a los municipios paraguayos por medio de redes móviles, mientras que las tecnologías cableadas de hogar tienen muy poca cobertura. En términos del uso de internet, el porcentaje de penetración, que se entiende como "la cantidad de personas que pueden acceder dentro de un país", se aproxima al 30%[3]. Apenas el 5% de los hogares cuenta con internet fijo[4]. Sin embargo, esta cifra asciende a un 25% de acceso cuando se refiere a telefonía móvil[5]. De hecho, internet por telefonía móvil tiene una cobertura amplia con redes de 2G/3G/4G, aunque la red 4G es aún muy limitada. Según datos de la Comisión Nacional de Telecomunicaciones (CONATEL), al final de 2014 Paraguay tenía 252.118 suscriptores de internet móvil y 185.125 suscriptores de internet fijo, con un total de 437.243 suscripciones en 6.802.295 de población total[6].

Por otro lado, cada vez más países en el mundo cuentan con mayor capacidad tecnológica para realizar vigilancia simultánea, invasiva, focalizada y de larga escala para interceptar comunicaciones[7]. Desde el momento de las relevaciones de Edward Snowden sobre la existencia de distintos programas nacionales e internacionales dirigidos por la Agencia Nacional de Seguridad (NSA) de Estados Unidos, destinados a vigilar en forma masiva las comunicaciones privadas de millones de usuarios de internet, se ha puesto en debate público el contexto y límites de lo que resulta válido sobre el monitoreo sistemático por parte de los Estados. En algunos casos esta vigilancia ha sido inducida por el discurso de la doctrina de seguridad nacional, colisionando con el sistema internacional de derechos humanos[8]. Un ejemplo de ello son las campañas del gobierno paraguayo que terminan por silenciar, reprimir y vigilar a todas las personas, en nombre de la lucha contra el tráfico de drogas o el terrorismo[9].

Otro peligro que atenta contra el derecho al acceso a la información y al conocimiento es la última modificación de la Ley 1328/98 de derechos de autor en Paraguay[10]. Esta modificación aumentó los derechos conexos sobre una obra, llevando su monopolio privado de 50 a 70 años luego de su fijación[11]. Estas políticas de proteccionismo a la industria cultural causan grandes daños, limitando la capacidad de creación de las personas y coartando su derecho a acceder a conocimiento y cultura[12].

Si bien la persecución de los hechos punibles y la seguridad nacional son legítimos, es importante que estos objetivos se limiten a la doctrina constitucional que es el acuerdo social por excelencia y garantía democrática para limitar la intromisión del Estado en la vida privada de las personas. A esto se suma el sistema internacional de derechos humanos que establece estándares y principios

3 Banco Mundial. *Indicadores del Desarrollo Mundial* (2009-2013).

4 Banco Mundial. Abonados a internet por banda ancha fija (por cada 100 personas), 2013. datos.bancomundial.org/indicador/IT.NET.BBND.P2/countries/PY?display=graph

5 Banco Mundial. Abonos a teléfonos celulares (por cada 100 personas), 2014. datos.bancomundial.org/indicador/IT.CEL.SETS.P2/countries/PY?display=graph

6 CONATEL. Suscriptores de internet móvil y fijo (2010-2014). www.conatel.gov.py/images/2015-2/PNT/DESARROLLO/midt%202014.pdf

7 La Rue, F. (2013, 17 abril). Informe del Relator Especial de las Naciones Unidas para la protección del derecho a la libertad de expresión y de opinión. Naciones Unidas, A/HRC/23/40, párr. 33. daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/06/PDF/G1313306.pdf?OpenElement

8 Por ejemplo: USA Patriot Act del 26 de setiembre de 2001, o la Ley orgánica de seguridad ciudadana, más conocida como "Ley mordaza" de España, por citar nada más un ejemplo fundante (la primera) y un ejemplo reciente y conocido (la segunda).

9 Polischuk, S. (2015, 9 marzo). Otro periodista asesinado en Paraguay mientras aumenta la vigilancia estatal. *Resumen Latinoamericano*. www.resumenlatinoamericano.org/2015/03/09/otro-periodista-asesinado-en-paraguay-mientras-aumenta-la-vigilancia-estatal

10 sil2py.senado.gov.py/formulario/VerDetalleTramitacion.pmf?q=VerDetalleTramitacion%2F1406

11 Sequera Buzarquis, M. (2013, 5 diciembre). ¿70 años de derechos conexos? No, gracias. *Tedic*. www.tedic.org/70-anos-de-derechos-conexos-no-gracias

12 El daño principal que puede ocasionar aumentar los derechos conexos en 20 años más es la pérdida de acceso a un sinnúmero de libros, periódicos, folletos, fotografías, películas, grabaciones y otras obras que son "propiedad" y que en gran medida ya no se comercializan. De esta forma se someten al olvido y a posible pérdida permanente. Los términos extendidos también son costosos para los consumidores e intérpretes, mientras que las personas que se benefician son los propietarios de las empresas tenedoras de los derechos conexos que muy probablemente no tengan nada que ver con la creación original de la obra.

para inhibir los riesgos y abusos de estos derechos fundamentales.

Paraguay cuenta con protecciones constitucionales y ratificaciones de convenciones internacionales sobre derechos humanos. Sin embargo esto no garantiza las salvaguardas adecuadas cuando el Estado se expande tecnológicamente en materia de vigilancia de las comunicaciones. La ausencia de regulación en la materia no atenta contra los derechos humanos *per se,* sino que dificulta la rendición de cuentas y el control ciudadano sobre la vigilancia estatal a través de las telecomunicaciones. Algunas de estas leyes que refuerzan la doctrina de la seguridad nacional y vulneran el sistema de derechos humanos se encuentran vigentes, mientras que otras están en estudio en el Congreso Nacional.

A pesar de lo citado anteriormente, existen importantes hechos de resistencia a violaciones de derechos humanos y profundización de garantías constitucionales en Paraguay. Un ejemplo de esto fue el rechazo y archivo en julio de 2015 del proyecto de ley que establecía la obligación de conservación de datos de tráfico[13] por parte de las proveedoras de internet. Esta fue una victoria política de la ciudadanía[14] que logró analizar, discutir y presionar a las autoridades para que rechazaran un proyecto que ponía en peligro el derecho a la privacidad de toda la población.

Asimismo, ha entrado en vigencia la Ley de acceso a información pública[15] a través de su decreto reglamentario[16]. Esta es una oportunidad para que la ciudadanía exija rendición de cuentas sobre las actividades que realiza el gobierno –en particular sobre aquellas que violentan los derechos fundamentales– y el libre ejercicio de las comunicaciones, garantías protegidas democráticamente y avaladas constitucionalmente.

13 Sistema de Información Legislativa: Proyecto de ley de retención de datos de tráfico. sil2py.senado.gov.py/formulario/VerDetalleTramitacion.pmf?q=VerDetalleTramitacion%2F102821

14 Campaña Pyrawebs: www.pyrawebs.tedic.org

15 Ley No. 5282 de libre acceso ciudadano a la información pública y transparencia gubernamental (2014). www.hacienda.gov.py/web-hacienda/archivos_de_disenho/imagenes/images/ley%205282.pdf

16 Decreto No. 4064 por el cual se reglamenta la Ley No. 5282/2014 de libre acceso ciudadano a la información pública y transparencia gubernamental (2015). www.idea.org.py/v1/wp-content/uploads/2015/09/DECRETO-4064-14.pdf

MARCO NORMATIVO GENERAL, REGULACIÓN MÁS IMPORTANTE SOBRE INTERNET EN EL PAÍS

El ordenamiento jurídico paraguayo tiene como norma suprema a la Constitución Nacional (CN), que en su artículo 137 la define ley superior a las que siguen de manera escalonada: "los tratados, convenios y acuerdos internacionales aprobados y ratificados, las leyes dictadas por el Congreso y otras disposiciones jurídicas de inferior jerarquía, sancionadas en consecuencia, integran el derecho positivo nacional en el orden de prelación enunciado (…)". Esto posiciona a los tratados y convenciones sobre derechos humanos por encima de leyes nacionales que sean menos favorables para las personas.

LA CONSTITUCIÓN NACIONAL

El artículo 33 de la CN sobre el derecho a la intimidad expone:

> La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas.

Este mismo artículo refuerza los demás derechos humanos que se encuentran en la CN: libertad de expresión y de prensa, derecho de acceso a la información pública, libertad de asociación y manifestación[17].

La privacidad de las comunicaciones se encuentra protegida en el artículo 36 de la CN del derecho a la inviolabilidad del patrimonio documental y la comunicación privada:

> El patrimonio documental de las personas es inviolable. Los registros, cualquiera sea su técnica, los impresos, la correspondencia, los escritos, las comunicaciones telefónicas, telegráficas o de cualquier otra especie, las colecciones o reproducciones, los testimonios y los objetos de valor testimonial, así como sus respectivas copias, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos específicamente previstos en la ley, y siempre que fuesen indispensables para el esclarecimiento de los asuntos de competencia de las correspondientes autoridades. La ley determinará modalidades especiales para el examen de la contabilidad comercial y de los registros legales obligatorios. Las pruebas documentales obtenidas en violación o lo prescrito anteriormente carecen de valor en juicio. En todos los casos se guardará estricta reserva sobre aquello que no haga relación con lo investigado.

De esta forma la CN establece como medida de intervención del Estado solo por orden judicial[18].

El primer derecho que se ve comprometido en el marco de las actividades de vigilancia de las comunicaciones en internet por las autoridades es el derecho a la privacidad. Este comprende el derecho de toda persona la protección de la información relacionada con su intimidad personal, es decir, que esta no sea objeto de acceso, registro o alteración por parte de terceros sin que medie autorización. Por lo tanto, cuando una autoridad lleva a cabo actividades destinadas a registrar, interferir o acceder a las comunicaciones de una persona, deberá ser de forma excepcional y contar con autorización judicial previa.

NORMAS INTERNACIONALES

La Declaración Universal de Derechos Humanos señala en su artículo 12 que nadie puede ser objeto de injerencias arbitrarias en su vida privada ni de su familia, su domicilio o correspondencia, y afirma además que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques[19].

En correspondencia, el derecho a la privacidad también se encuentra reconocido en los artículos 11 de la Convención Americana sobre Derechos Humanos[20] y 17 del Pacto Internacional de Derechos Civiles y Políticos[21].

17 Constitución Nacional, Artículos 26, 28, 29, 32. jme.gov.py/transito/leyes/1992.html

18 Ver, por ejemplo, la acción de inconstitucionalidad en el juicio: "Juan Claudio Gaona Cáceres y Ruben Melgarejo Lanzoni s/ soborno, extorsión en grado de tentativa, cohecho pasivo agravado". Año 2008 – No. 799 – Corte Suprema de Justicia, Sala Constitucional. "En materia de intervención de comunicaciones telefónicas autorizadas por resolución judicial, no puede confundirse el distinto alcance que arrastra la vulneración de derechos constitucionales con la infracción, como medio probatorio de cargo, sin perjuicio que puedan cumplir una finalidad como fuente de investigación, puedan vulnerar la legalidad constitucional produciéndose de esta forma su nulidad con los efectos que ella acarrea". www.csj.gov.py/jurisprudencia/cache/25c136e078225ec4be3ff3ec67d4b407.htm

19 Declaración Universal de Derechos Humanos. www.un.org/es/documents/udhr

20 Convención Americana sobre Derechos Humanos. www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.htm

21 Pacto Internacional de Derechos Civiles y Políticos. www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

LEYES NACIONALES

El Congreso paraguayo ha adoptado otras leyes con la finalidad de proteger datos personales, incluyendo la Ley 1682/01, que fue posteriormente modificada por la Ley 1962/02[22]. Esta ley sobre datos personales tiene grandes limitaciones que incluyen conceptos vagos e imprecisos sobre cuáles son datos sensibles. Tampoco tiene un alcance satisfactorio, ya que no aplica a las bases de datos construidas por entes públicos y/o privados. A su vez no cuenta con una autoridad responsable de protección de datos. Todo esto significa que cada individuo debe presentar de forma unilateral acción de *habeas data* por cada caso de violación a dicha ley. También se encuentran falencias en la protección de datos sensibles como "condición médica", ya que no impone sanción alguna por violaciones en el manejo de información sobre la salud personal. Solamente están previstas sanciones para los casos de violaciones de datos sobre solvencia económica y financiera.

Un ejemplo reciente de flagrante violación de la confidencialidad y la privacidad del paciente fue el caso del embarazo de una niña de 10 años ocurrido en Paraguay en mayo del 2015[23]: su condición de salud fue de conocimiento público desde que el caso salió a la luz hasta el momento mismo del parto. Por otro lado, varios órganos de tratados de las Naciones Unidas, como el Comité para la Eliminación de la Discriminación contra la Mujer (CEDAW) se han mostrado preocupados sobre los casos de mujeres que ingresan en hospitales por complicaciones de abortos[24]. En estos casos también se hacen públicos los datos personales de las mujeres que abortaron.

El *habeas data* se encuentra dentro de las garantías constitucionales (artículo 133 de la CN). El caso más emblemático en materia de *habeas data* fue la acción interpuesta por el Sr. Martín Almada en 1992[25], quien a través del derecho de *habeas data* logró descubrir los archivos secretos de la policía de la dictadura militar de Alfredo Stroessner (1954-1989) conocido como el "Archivo del Terror"[26]. En la actualidad, el recurso de *habeas data* se instaura ante un juez de primera instancia.

Además, el Código Penal establece, en virtud del Capítulo VII de hechos punibles contra la vida privada y la intimidad de la persona, otras sanciones penales por varias violaciones incluyendo: violación del domicilio (artículo 141), *trespassing* (artículo 142), daño a la privacidad de una persona (artículo 143), daño al derecho a la comunicación e imagen (artículo 144), violación de la confidencialidad (artículo 145), violación del secreto de las comunicaciones (artículo 146), revelación de secretos privados de una persona con una especial obligación de mantener el secreto debido a su profesión (artículo 147, 148) y revelación de secretos privados con fines económicos (artículo 149).

El Código Procesal Penal describe los mecanismos y las reglas necesarias para perseguir los delitos. En virtud de los artículos 198 y 199 se permite mediante orden judicial la interceptación e incautación de la correspondencia, telégrafo o cualquier otro tipo de correspondencia. El artículo 200 del mismo texto mantiene la posibilidad de vigilancia de las comunicaciones con carácter excepcional, y establece que un juez puede ordenar la interceptación de las comunicaciones de personas acusadas de delitos, utilizando cualquier mecanismo técnico necesario para obtener la

22 Su primer artículo expresa: "Esta ley tiene por objeto regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares. No se aplicará esta Ley en ningún caso a las bases de datos ni a las fuentes de informaciones periodísticas ni a las libertades de emitir opinión y de informar". Es decir, queda prohibida la publicación o difusión de datos personales "sensibles" mientras que es lícita la recolección, almacenamiento, procesamiento y publicación de datos o características personales, que se realicen con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudio de mercado. Existe un proyecto de modificación de los artículos 5 y 9 que se encuentra en discusión en el Congreso Nacional. La Nación. (2015, 18 agosto). Diputados ratifican sanción a Ley de Informconf. *La Nación*. www.lanacion.com.py/2015/08/18/diputados-ratifican-sancion-a-ley-de-informconf

23 ABC. (2015, 18 agosto). Niña dará a luz mañana. *ABC*. www.abc.com.py/nacionales/nina-dara-a-luz-mana-na-1396977.html

24 Comité para la Eliminación de la Discriminación contra la Mujer (2011, 8 noviembre). Observaciones finales del Comité para la Eliminación de la Discriminación contra la Mujer – Paraguay. CEDAW/C/PRY/CO/6. docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhss1YTn0qfX85YJz37paIgUBwjoBC6j%2bb4e1uJXjFZmv93DCaJG9sGnY62ywUjHPxZhm%2ffbkxDRUvGYN5y%2bvkMs%2fIndxu6R7%2fTbra2TzNqfS1

25 El 14 de septiembre de 1992, a las 8:10 horas, ante el juzgado de Primera Instancia Criminal del Tercer Turno, se presentó una solicitud de *habeas data* por el Dr. Martín Almada, bajo patrocinio de los abogados Pedro Darío Portillo y Rodolfo Aseretto. www.pj.gov.py/contenido/132-museo-de-la-justicia/132

26 El archivo conocido como el "Archivo del Terror" del Plan Cóndor registra las operaciones de la policía secreta de Stroessner durante décadas. Contiene información sobre la coordinación de operaciones con las dictaduras vecinas, en particular con Chile y Argentina. Esta revelación demostró que los mecanismos de vigilancia de Stroessner estaban vigentes incluso después de haber sido derrocado en 1989.

información necesaria para la investigación. Pero no queda suficientemente claro los límites de qué tipo de tecnología deberá ser utilizada y cuán desmedido puede ser su uso afectando desproporcionalmente un cúmulo de derechos fundamentales del individuo sospechoso.

Por otra parte, la Unidad Especializada en Delitos Informáticos –unidad que intentó comprar software de vigilancia de la compañía italiana Hacking Team– según las resoluciones No. 3459/10 y 4408/11, tiene facultades de pedir a un juez la intervención de comunicaciones en la investigación ciertos delitos específicos, como acceso indebido a datos, interceptación, preparación al acceso indebido a datos, alteración de datos o a sistemas informáticos, sabotaje a sistemas informáticos, falsificación de tarjetas, entre otros.

El Ministerio Público, en términos generales, puede acceder a las comunicaciones intervenidas una vez que el juez brinde la autorización correspondiente. En el artículo 89 de la Ley de telecomunicaciones 642/95 se establece la protección e inviolabilidad en los servicios de telecomunicaciones con la excepción de que exista orden judicial del juez competente[27]. El artículo 90 por su parte, robustece el significado de la inviolabilidad, que ocurre cuando una persona que no es el receptor original de la comunicación tiene conocimiento de la existencia o el contenido de la comunicación y tiene la oportunidad de sustraer, interferir, cambiar el contenido o el itinerario, publicar o utilizar dicha información. A esta ley se agrega el decreto del Poder Ejecutivo 14135/96, que la complementa a través de su artículo 9 sobre la inviolabilidad y el secreto de las telecomunicaciones[28].

El principio de "neutralidad de la red" es un componente relevante para el ejercicio de la libertad de expresión y privacidad en internet. Paraguay cuenta con la resolución 190/2009[29] de la Comisión Nacional de Telecomunicaciones (CONATEL) que expresa la protección de este principio en su artículo 26: "El prestador que provea el servicio deberá respetar el principio de neutralidad de las redes; por el que no podrá interferir o degradar el tráfico recibido o generado por el usuario, ni variar la capacidad contratada según el tipo de contenido, aplicación, origen o destino decidido por él". Sin embargo, en ninguna parte del reglamento ni en los anexos existen sanciones punitivas o administrativas en el caso de que se incurra en alguna falta. Igualmente, la ciudadanía ha tomado conciencia de la importancia de este principio y ha elevando quejas contra aquellas proveedoras que cometen infracciones de este principio y su correspondiente artículo de la resolución. Un caso emblemático de violación al principio de neutralidad fue el bloqueo de una proveedora de internet al sitio satírico ABC.me por motivos particulares[30], muestra de que los abusos no solo son cometidos por los Estados. Si bien la regulación se encuentra en una resolución, actualmente el proyecto de modificación de la Ley de telecomunicaciones la elevaría al rango de ley. Desafortunadamente, la propuesta no cuenta con penas restrictivas o privativas de reclusión y multas cuando se incurre en la violación de este principio.

Cabe destacar que no todas las regulaciones de CONATEL cumplen con los estándares de derechos humanos, incurriendo algunos casos en contradicciones con la CN o los tratados internacionales. Por ejemplo, el reglamento de CONATEL 1350/2002[31] pone en riesgo las comunicaciones de las personas ya que en su artículo 1 establece: "el plazo de seis (6) meses, como periodo obligatorio de conservación del registro de detalles de llamadas entrantes y salientes de todas las líneas que conforman la cartera de clientes de las diferentes operadoras del servicio de telefonía móvil celular (STMC) y/o Sistema de Comunicación Personal (PCS)". No hay penas administrativas y restrictivas o multas en caso de difusión pública o privada del contenido de esas señales.

27 Véase Artículo 89 de la Ley de telecomunicaciones 642/95.

28 El artículo 9 establece que: "Se atenta contra la inviolabilidad y el secreto de las telecomunicaciones, cuando deliberadamente una persona que no es la que efectúa la comunicación ni es la destinataria, sustrae, intercepta, interfiere, cambia o altera su texto, desvía su curso, publica, utiliza, trata de conocer o facilitar que él mismo u otra persona, conozca la existencia o el contenido de cualquier comunicación. Las personas que en razón de su función tienen conocimiento o acceso al contenido de una comunicación efectuada a través de los servicios de telecomunicaciones, están obligadas a preservar y garantizar la inviolabilidad y el secreto de la misma. Los concesionarios o licenciatarios y autorizados a prestar o utilizar servicios de telecomunicaciones, están obligados a adoptar las medidas más idóneas para garantizar la inviolabilidad y el secreto de las comunicaciones efectuadas a través de tales servicios".

29 Comisión Nacional de Telecomunicaciones. (2011). Resolución Directorio W 190/2009, Reglamento de los servicios de acceso a internet, transmisión de datos. https://webcache.googleusercontent.com/search?q=cache:q5EXMXB7Lp8J:docs.paraguay.justia.com/nacionales/leyes/resolucion-n-190-del-11-de-marzo-de-2009-por-la-cual-se-establece-el-reglamento-de-los-servicios-de-acceso-a-internet-transmision.doc+&cd=5&hl=es&ct=clnk&client=ubuntu-browser

30 El caso ABC.me fue una parodia sobre medio de difusión ABC que provocó el bloqueo de dicha web durante cuatro horas por parte de las PSI locales. También fue notoria la protesta contra el bloqueo de llamada a través de Whatsapp. Ambos casos obligaron a CONATEL a tomar una posición al respecto. Más información: www.tedic.org/las-continuas-violaciones-a-la-neutralidad-de-la-red-en-paraguay

31 Comisión Nacional de Telecomunicaciones (CONATEL). (2002, 6 noviembre). Resolución No. 1350/2002. www.buscoley.com/pdfs/r_1350_2002.pdf

Otra normativa que pone en riesgo la privacidad de las comunicaciones y que colisiona con la CN es la Ley 4868/13 de comercio electrónico, que en su artículo 10[32] obliga a las empresas proveedoras de internet en Paraguay y proveedores de servicios de alojamiento de datos a almacenar los datos de tráfico o "relativos a la comunicaciones electrónicas" por seis meses. Esta ley no cumple los estándares mínimos para salvaguardar la información privada de los usuarios, ni criterios claros sobre cuáles son los datos que se podrán almacenar y cuáles no. Cabe destacar que el artículo 10 prohíbe al Poder Judicial y a la Policía Nacional acceder a estos datos almacenados por las empresas.

Desde 2014, Paraguay cuenta con un Sistema de Inteligencia Nacional, creado por el Presidente de la República Horacio Cartes a través del Decreto Presidencial No. 2812 del 18 de diciembre de ese año[33] que reglamenta la Ley No. 5241 del 22 de agosto. En el artículo 14 de dicha ley y el artículo 12 del decreto solo el Sistema Nacional de Inteligencia (SINAI) tiene la autoridad para "recopilar y procesar" información con el objetivo de salvaguardar la seguridad de la nación.

Sin embargo, el artículo 24 de mismo decreto establece que la Dirección General de Inteligencia es también responsable de la recolección y tratamiento de la información para producir inteligencia. Llama mucho la atención que esta Dirección no aparece en la Ley No. 5241/2014 ni tampoco se mencionan sus actividades y atribuciones.

Si bien la ley establece que la vigilancia de las comunicaciones se realizará solamente en circunstancias excepcionales –es decir, si no se puede obtener en otro lugar en virtud del artículo 24, y por autorización judicial en virtud del artículo 26– las siguientes áreas son motivo de preocupación porque existe la necesidad de garantizar la aplicación de las normas de derechos humanos para la vigilancia de las comunicaciones por parte de estas agencias de inteligencia. De cualquier manera, no es legítimo justificar la vigilancia de las comunicaciones bajo el concepto de "recolección de inteligencia" ya que el texto de la regulación no define qué es "inteligencia" y cuán desproporcionada puede ser esta vigilancia, que pueden afectar a personas que incomoden al actual gobierno, como son políticos opositores, periodistas y activistas, entre otros[34].

La ley establece que la inteligencia será englobada en el SINAI y se utilizará para prevenir, alertar e informar de cualquier amenaza o riesgo que afecte a los intereses nacionales (artículo 2a). Esta es una definición muy amplia y vaga que no puede limitar el propósito y objetivo de la vigilancia de la comunicación y abre la puerta a diferentes tipos de abusos.

El artículo 4 describe los principios por los cuales el SINAI, incluyendo los organismos e individuos que lo componen, tendrá que solicitar autorización judicial para obtener información de carácter personal. Sin embargo, el artículo también establece los casos en que esta autorización judicial no será necesaria, a saber: casos de amenazas "graves", o aquellos que pongan en riesgo la seguridad colectiva, o la seguridad de autoridades e instituciones, o los que atenten contra la seguridad pública y el Estado de Derecho. Al no definir lo que constituye "grave", esto se convierte en una amplia oportunidad de eludir legalmente la exigencia de autorización judicial.

Otra oportunidad de violar las comunicaciones la brinda la Ley No. 1881 que modifica la Ley No. 1340 del 22 de noviembre de 1988 "Que reprime el tráfico ilícito de estupefacientes y drogas peligrosas y otros delitos afines y establece medidas de prevención y recuperación de farmacodependientes". Esta ley otorga a la Secretaría Nacional Antidrogas (SENAD) la potestad de interceptar, registrar, grabar las comunicaciones orales, cablegráficas o electrónicas a través de la solicitud de un juez, que podrá autorizar en cada caso y por tiempo determinado.

Incluso existen problemas a nivel de lo que se conoce como propiedad intelectual. El Artículo 184 del Código Penal, Ley No. 1160/97[35] expresa que la violación de los derechos de autor será sancionada con pena privativa de libertad de hasta tres años o multa a la persona que sin autorización del titular divulgue, promocione, reproduzca o represente públicamente una obra protegida por la ley de derecho de autor. Esta ley se aplica en el entorno en línea con todas las complejidades que esto representa, como la forma de obtención de la información a través de la vigilancia previa: IP de la descarga ilegal o la incautación de la computadora o teléfono celular, lo que afecta desproporcionadamente a los derechos fundamentales.

ANTEPROYECTOS DE LEYES QUE PODRÍAN AFECTAR LOS DERECHOS FUNDAMENTALES EN INTERNET

Existen dos proyectos de ley que pueden afectar los derechos fundamentales en internet que se encuentran actualmente en estudio por parte del Congreso Nacional.

32 www.eljurista.com.py/admin/publics/upload/archivos/ea-41b40fb8ce27bd7ec64237fd75ef89.pdf

33 www.presidencia.gov.py/archivos/documentos/DECRETO2812_uegnk41y.pdf

34 ONU, Asamblea General. (2014, 21 enero). Resolución aprobada por la Asamblea General el 18 de diciembre de 2013 [sobre la base del informe de la Tercera Comisión (A/68/456/Add.2)] 68/167. El derecho a la privacidad en la era digital. A/RES/68/167. www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167&referer=http://www.un.org/depts/dhl/resguide/r68_resolutions_table_en.htm&Lang=S

35 www.mre.gov.py/v1/Adjuntos/Privacidad/Ley1160.pdf

El proyecto de ley de protección de niños y adolescentes contra contenidos nocivos de internet[36] pretende regular el filtrado de contenidos en internet en redes inalámbricas públicas e incluso a nivel de los PSI[37].

Por otro lado, el proyecto de ley sobre crimen organizado otorga atribuciones no usuales a los agentes estatales que se encargan de este tipo de investigaciones. Según el jurista Jorge Rolón Luna[38], quien analizó este proyecto, se establece claramente cuáles son los delitos a los que se aplicará estas técnicas especiales de investigación: es una lista bastante amplia que incluye 17 tipos penales del Código Penal. Además se aplicará en conjunto con otras leyes "especiales" como ser: lucha contra el narcotráfico[39], la trata de personas prevista en el Código Aduanero[40], la Ley de armas de fuego[41], la Ley antiterrorista[42] y otras leyes penales[43]. Se establece que como parte de las investigaciones de este tipo de delitos, se podrá realizar "vigilancia electrónica", definida de la siguiente manera:

> La vigilancia electrónica es la técnica especial de investigación que permite la utilización de todos los medios tecnológicos y/o electrónicos conocidos o a conocerse, que permitan obtener información y elementos de prueba con respecto a la comisión del hecho punible investigado o que permitan identificar a los autores y partícipes.

36 sil2py.senado.gov.py/formulario/VerDetalleTramitacion.pmf?q=VerDetalleTramitacion%2F103933

37 Artículo 3. De la protección activa: "Los proveedores de servicios de internet (ISP) deberán brindar e instalar de manera obligatoria y gratuita, a sus clientes y usuarios, los cuales deberán declarar al momento de suscribir el correspondiente contrato de prestación de servicios, o en cualquier momento posterior, si niñas, niños o adolescentes tendrán acceso a internet, o a cualquiera que lo solicite, un software específico con sistemas de detección, filtro, clasificación, eliminación y bloqueo de contenidos no aptos de conformidad al artículo 2, con los respectivos manuales e indicaciones para su uso".

38 Jorge Rolón Luna, jurista, ex magistrado (1996-2002), ex comisionado en el Mecanismo Nacional de Prevención contra la Tortura en Paraguay (2012-2015).

39 Ley 1340 del 22 de noviembre de 1988 que reprime el tráfico ilícito de estupefacientes y drogas peligrosas y otros delitos afines y establece medidas de prevención y recuperación de farmacodependientes y sus modificatorias.

40 Ley 2422/04, Código Aduanero.

41 Ley 4036/10 de armas de fuego, sus piezas y componentes, municiones, explosivos, accesorios y afines.

42 Los previstos en la Ley 4024/10 que castiga los hechos punibles de terrorismo, asociación terrorista y financiamiento del terrorismo.

43 Ley 4439/11 que modifica y amplía varios artículos de la Ley 1160/97 Código Penal y la Ley 3440/08 que modifica varias disposiciones de la Ley 1160/97, Código Penal.

CASOS PROBLEMÁTICOS

Actualmente no existe jurisprudencia en lo que respecta a los derechos fundamentales en el entorno en línea como la prohibición explícita del uso de cifrado o anonimización que afectan directamente a la libertad expresión. Sin embargo, existe información sobre la compra de diversas tecnologías destinadas a interceptar las comunicaciones que incluyen las redes e internet. Esto afecta no solo la privacidad, sino el derecho a la libertad de opinión y libertad de asociación, generando una intromisión indirecta a la faceta individual de la persona. Uno de los casos ya mencionados que atentó contra el principio de neutralidad en internet sucedió cuando dos empresas prestadoras de servicios –Personal y Tigo– bloquearon arbitrariamente el acceso al sitio humorístico ABColor.me en 2012. La censura corporativa puede ser tan perniciosa como la estatal y, en algunos casos, más poderosa. Ante esta situación no hubo ningún pronunciamiento ni sanción por parte de CONATEL, el ente regulador de las telecomunicaciones. De todos modos, la ciudadanía hizo eco de esta contrariedad y luego de pocas horas se resolvió el inconveniente[44].

Otro ataque contra la neutralidad de la red es el que viene haciendo la proveedora Tigo desde 2013, ofreciendo a sus usuarios el acceso gratuito a la red social Facebook[45]. Esta experiencia ha sido destacada positivamente por Mark Zuckerberg en diversas declaraciones públicas en el marco del proyecto internet.org[46]. Aunque esta alianza entre Tigo y Facebook atenta contra la neutralidad y tiene los mismos inconvenientes que el propio proyecto internet.org, CONATEL no se ha pronunciado al respecto, como sí lo hizo en el caso del bloqueo de llamadas de WhatsApp[47].

La compra de software de seguridad por parte del Estado es otro caso problemático. El llamado a licitación pública a través del Ministerio del Interior para dicha compra[48], en su pliego de bases y condiciones, no describe las características especiales del software por razones de confidencialidad. El Congreso Nacional ha solicitado informes al respecto pero aun se desconoce la respuesta[49]. Las escuchas telefónicas sin orden judicial también son una realidad en el país aunque, según un representante del Ministerio del Interior, se utilizarán única y exclusivamente para los casos de extorsión y secuestro[50].

Asimismo, ha surgido una serie de publicaciones filtradas por Wikileaks[51] sobre el Ministerio del Interior. Se demuestra que durante la administración de Fernando Lugo, el entonces Ministro Rafael Filizolla mantuvo conversaciones con la embajada de los Estados Unidos, para dar explicaciones sobre el nuevo programa de interceptación del gobierno, incluyendo la telefonía celular. Se desconoce las características de este sistema, así como su uso efectivo en la persecución de hechos punibles.

Las escuchas telefónicas son hechos ya denunciados en varias oportunidades y ante las instituciones de persecución penal. Sin embargo, también aquí desconocen los resultados de las investigaciones y todo está cubierto por un manto de silencio. El Congreso Nacional se vio afectado por este tipo de abusos y ha puesto esta situación en debate en el actual ejercicio[52].

44 www.tedic.org/roben-este-post-neutralidad-en-la-red

45 ABC. (2013, 4 diciembre). Facebook móvil gratis para clients de Tigo. *ABC*. www.abc.com.py/abc-tv/locales/facebook-movil-gratis-para-clientes-de-tigo-646280.html

46 ABC. (2014, 25 febrero). Zuckerberg destaca ejemplo de Paraguay. *ABC*. www.abc.com.py/ciencia/zuckerberg-destaca-ejemplo-de-paraguay-1218676.html

47 Sequera Buzarquis, M. (2014, 21 enero). ¿Tigo y Personal atentan la Neutralidad en la Red? [Derechos Digitales]. Tedic. www.tedic.org/tigo-y-personal-atentan-la-neutralidad-en-la-red-derechos-digitales

48 Licitación pública nacional No. 17/2013 "Adquisición de equipamientos y periféricos para la seguridad interna plurianual" (Policía Nacional). Página 10. www.contrataciones.gov.py/sicp/download/getFile?cid=45685&fileName=OAwkXiYNi6QOh%2BTIKqR3782C1d%2Fp2D6FjIiEs6npdi%2F1ZqqfT7VKyeTQxatNaWt5IxSb9jusPNXO1wj6SydKziVsfoYTRYq%2BBaCsYn4it67q6WhpQnEfFfcXrCqQvEbOmkkgUBngwr4ij3Ea4EbM7A%3D%3D

49 www.agendalegislativa.com.py/senado/5922-senado-pide-informe-al-ministerio-del-interior-sobre-equipos-de-escuchas-telefonicas

50 Telefuturo Paraguay, Informe Canal 4. (2014, 26 noviembre). Escuchas telefónicas sin orden judicial se darán en caso de extorsión y secuestro. www.youtube.com/watch?v=3Bkdspxhae8

51 WikiLeaks. (2010, 18 febrero). GoP seeks to implement new cell phone intercept system, but promises to keep SIU program intact. https://wikileaks.org/plusd/cables/10ASUNCION97_a.html

52 EFE. (2014, 25 noviembre). Convocan a ministros y a fiscal general por escuchas telefónicas a legisladores. *Última Hora*. www.ultimahora.com/convocan-ministros-y-fiscal-general-escuchas-telefonicas-legisladores-n850778.html; Escuchas telefónicas fiscales. (2003, 10 noviembre). *ABC*. www.abc.com.py/edicion-impresa/policiales/escuchas-telefonicas-a-fiscales-729970.html

El debate sobre este asunto se intensificó ante las diversas apariciones de la situación paraguaya en la prensa internacional, sobre las compras de tecnología para la vigilancia masiva a través de internet. Destacan las conversaciones que mantuvo el fiscal de delitos informáticos, Ariel Martínez, con la empresa Hacking Team[53], que se filtraron por WikiLeaks[54] y provocaron la atención mediática. El producto estrella de Hacking Team es un software que permite interceptar computadores, llamadas por Skype, correos electrónicos, mensajes instantáneos y contraseñas: se denomina Sistema de Control Remoto. Según la investigación de Privacy International[55], el software es capaz de eludir el cifrado de los programas de comunicación y registrar llamadas, ver el historial de navegación web, archivos y fotos eliminadas del dispositivo. Además, es capaz de tomar control de micrófonos y cámaras y usarlos para realizar espionaje. Afortunadamente la compra no se concretó[56].

Otro proceso de compra de tecnología de vigilancia fue el caso FinFisher[57]. La publicación de este caso la realizó CitizenLab –el laboratorio multidisciplinario de la Universidad de Toronto– a través del cual se pudieron conocer usos del software FinFisher[58]. El informe cita a Paraguay como uno de los países que han adquirido este software y explica que su funcionamiento es similar al que promociona la empresa italiana Hacking Team. El informe remarca desconocimiento sobre qué institución está gestionando esta herramienta de vigilancia. Sin embargo, el Centro de Respuestas ante Incidentes Cibernéticos de la Secretaría Nacional de Tecnologías de la Información y Comunicación (CERT de SENATICs) ha realizado una publicación oficial a través de su página web[59] explicando que se ha comunicado con CitizenLab y que la actividad de FinFisher se encuentra en observación ya que la misma es considerada un delito en Paraguay[60].

Otro elemento a tener en cuenta es el Plan Nacional de Ciberseguridad, que se terminó de redactar en junio de 2015, como propuesta de trabajo de implementación por parte del CERT de SENATICs con el apoyo del equipo técnico de la OEA[61]. En este programa contribuyen Canadá, Estados Unidos, Estonia y el Reino Unido. Además, actualmente Paraguay ejerce la presidencia del Comité Interamericano contra el Terrorismo y fue invitado a participar en la Convención de Budapest[62]. Se precisa mayor debate y discusión pública sobre la elaboración e implementación desde la perspectiva de los derechos fundamentales.

En lo que refiere al derecho de autor aplicado en internet, en Paraguay no existen casos de violación llevados a la justicia. Uno de los proyectos que podría haber impactado en esta área fue el archivado proyecto de retención de datos de tráfico[63] –proyecto Pyrawebs– que pretendía registrar todos los datos de tráfico en internet para perseguir cualquier hecho punible. Por lo tanto, la descarga no autorizada de contenidos con derecho de autor, podría caer dentro de la órbita de aplicación de esta ley. Gracias a una fuerte presión ciudadana la misma no fue aprobada.

53 www.hackingteam.it

54 Wikileaks. (2015, 8 julio). Hacking Team. Paraguay-Uruguay Report. https://wikileaks.org/hackingteam/emails/emailid/249535

55 Privacy International Report. Briefing for the Italian Government on Hacking Team's surveillance exports. (s/f) www.privacyinternational.org/sites/default/files/Briefing%20for%20the%20Italian%20Government%20on%20Hacking%20Team's%20surveillance%20exports.pdf

56 ABC. (2015, 9 julio). Gobierno negoció espionaje. *ABC.* www.abc.com.py/nacionales/estado-negocio-espionaje-1385872.html

57 Spyfile Wikileaks – FinFisher https://wikileaks.org/spyfiles4/customers.html

58 The Citizen Lab. (2015, 15 octubre). Pay no attention to the server behind the proxy: Mapping FinFisher's continuing proliferation. https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation

59 CERT-PY. (s/f) Finfisher y su relación con Paraguay. www.cert.gov.py/index.php/noticias/finfisher-y-su-relacion-con-paraguay (verificado el 9 de febrero de 2016).

60 Ver tuit oficial del CERT- SENATICs: https://twitter.com/CERTpy/status/697104856352428033 (verificado el 9 de febrero de 2016).

61 Paraguay recibe apoyo de la OEA para su Plan Nacional de Ciberseguridad. www.senatics.gov.py/noticias/-/asset_publisher/T0yoqne5nEay/content/paraguay-recibe-apoyo-de-la-oea-para-su-plan-nacional-de-ciberseguridad;jsessionid=818E970B5A4E7DC1209E014893EA278C

62 Voz de América. (2015, 7 mayo). OEA apoya plan de ciberseguridad de Paraguay. *Voz de América.* www.voanoticias.com/content/oea-ciberseguridad-paraguay/2753821.html

63 El proyecto Pyrawebs. Ver campaña www.pyrawebs.tedic.org

CONCLUSIONES Y RECOMENDACIONES

El debate sobre el derecho a la privacidad y la libertad de expresión en el ámbito digital es cada vez más relevante en Paraguay como en el resto de la región. Esto se debe al aumento de la conectividad que lleva a una mayor participación de las personas en el ámbito en línea, expresando y compartiendo sus puntos de vista y ejerciendo sus derechos. Esto también implica riesgos de ser perseguidos injustamente o intimidados, e incluso aplastados por el aparato estatal, empresas privadas, o grupos delictivos. Por ello deben establecerse políticas públicas que provean un mayor equilibrio y protejan aún más los derechos consagrados en la carta magna, ante las leyes y los proyectos que buscan invadir la libertad y la vida privada de las personas con la excusa de perseguir a los "jinetes del Apocalipsis".

Por otro lado, las crecientes regulaciones y castigos no son capaces de dar respuestas a las tensiones que se generan entre el derecho de acceso a la cultura y los derechos de autor y conexos. Existen nuevas formas de producir y de consumir bienes inmateriales promovidas por las velocidades de acceso y copia que proveen las redes y en particular internet. Las leyes deben buscar nuevos mecanismos de proteger o fomentar la creación sin convertirse en "jaulas de acero" que dificulten el acceso a la cultura.

Creemos que hay que construir nuevas bases que reconozcan estas nuevas formas y esta nueva herramienta llamada "internet": que se incluyan los nuevos hábitos de hacer cultura a través de las tecnologías de información y comunicación y que protejan a los usuarios de los abusos de las corporaciones y los estados ante las vigilancias desproporcionadas e innecesarias, para de esta forma resguardar el patrimonio inmaterial que es la cultura.

Otra cosa que resulta interesante para el caso paraguayo es que no se cuenta con entidades autorizadas para intervenir las comunicaciones privadas sin orden judicial de acuerdo con el orden jurídico vigente. No es posible que una prueba obtenida ilegalmente, como por ejemplo la interceptación ilegal de una comunicación, sea subsanada *a posteriori* por un juez. De acuerdo con los artículos 166, 168 y 169 del Código Procesal Penal, situaciones como esas son causales de nulidades absolutas que no pueden ser saneadas y mucho menos convalidadas.

Necesitamos un mayor debate para la aplicación de cualquier tipo de plan o programa que no incluya la perspectiva de los derechos humanos, como por ejemplo el Plan de Ciberseguridad. Este mecanismo deberá ser implicado también en el anteproyecto de modificación de la Ley de telecomunicaciones, donde no cuenta con penas restrictivas o privativas de reclusión y multa; las penas aumentan si existe difusión pública o privada del contenido de esas señales.

Sobre la modificación impostergable de la Ley de datos personales, en mi opinión esta es una materia de tratamiento urgente en el Congreso Nacional, que deberá ser llevada a un plano más profundo de discusión. Por un lado, la necesidad de una ley genuina, que incluya los elementos mínimos que fueron remarcados en este documento, y por el otro, que sea generada en torno a una agenda pública de debate. De todo esto se esperaría como resultado una regulación robusta y eficiente que sirviera de piedra angular en la defensa de los derechos fundamentales y evitar así que se generen leyes sin considerar estándares de protección de los derechos humanos, como por ejemplo el proyecto "Pyrawebs".

Otras normativas clave para fortalecer la libertad de expresión en Paraguay son la Ley de medios para proteger a las voces de periodistas y creadores de opinión y un marco civil de internet para reforzar los mecanismos de protección de derechos humanos e internet.

Paraguay se expande tecnológicamente con sistemas avanzados de vigilancia de las comunicaciones, sin las salvaguardas adecuadas: ausencia de regulaciones que obliguen a una rendición de cuentas; transparencia con respecto al uso y alcance de los poderes y técnicas de vigilancia de las comunicaciones; reportes de transparencia tanto en el proceso penal como de inteligencia. Además, no se cuenta con un órgano supervisor e independiente que autorizaría los casos de vigilancia tanto en los procesos penales como los de inteligencia nacional. Tampoco existen mecanismos de notificación diferida al usuario afectado en el proceso penal ni de inteligencia, con el objeto de que la ciudadanía pueda ejercer un control democrático acerca del ejercicio por parte de la autoridad de tales facultades.

APC
ASOCIACIÓN PARA
EL PROGRESO DE
LAS COMUNICACIONES

Internet y TIC para la justicia social y el desarrollo

APC es una red internacional de organizaciones de la sociedad civil fundada en 1990 que empodera y asiste a gente que trabaja por la paz, los derechos humanos, el desarrollo y la protección del medio ambiente, a través del uso estratégico de las tecnologías de información y comunicación (TIC).

APC trabaja para construir un mundo en donde todas las personas tengan un acceso fácil, equitativo y accesible al potencial creativo de las tecnologías de información y comunicación para mejorar sus vidas y crear sociedades más igualitarias y democráticas.

www.apc.org info@apc.org

Diseño gráfico: MONOCROMO

Escrito por Maricarmen Sequera Buzarquis

Encargado por la Asociación de Tecnología, Educación,
Desarrollo, Investigación, Comunicación (TEDIC)

ESTE INFORME SE HA ELABORADO COMO PARTE DEL PROYECTO EXAMINANDO LOS DERECHOS
Y LAS LIBERTADES EN INTERNET EN LATINOAMÉRICA (EXLILA)
DE LA ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES (APC).

EL PROYECTO ESTÁ FINANCIADO POR OPEN SOCIETY INSTITUTE (OSI) Y APC
Y ESTÁ COORDINADO POR LA ONG DERECHOS DIGITALES.

INFORME NACIONAL PARAGUAY
Marzo 2016

ISBN 978-92-95102-55-2 APC-201603-CIPP-R-ES-DIGITAL-246