LA DESPROTECCIÓN DE LOS DATOS PERSONALES Y LA DESIGUALDAD DE GÉNERO, RIESGOS A LAS LIBERTADES DE LAS PERSONAS EN INTERNET

DERECHOS DIGITALES

El análisis de la legislación y hallazgos de investigaciones sobre el manejo de datos en entes públicos y privados revelan que urge fortalecer estándares de protección de datos personales en Paraguay. También son necesarias políticas públicas que apunten a superar la brecha digital en términos de acceso y de uso para superar desigualdades.

Maricarmen Sequera y Jazmín Acuña
TECNOLOGÍA Y COMUNIDAD (TEDIC)

Introducción

La protección y el ejercicio de los derechos de las personas se trasladan al entorno en línea. En este espacio se cometen abusos y se perpetúan desigualdades que ponen en riesgo libertades fundamentales como la privacidad, la libertad de expresión y el acceso a información en igualdad de condiciones. Este artículo se centra en el estado del derecho a la privacidad con enfoque en la protección de datos personales en Paraguay y la situación de las mujeres en Internet.

El análisis de la legislación y hallazgos de investigaciones sobre el manejo de datos en entes públicos y privados revelan que urge fortalecer estándares de protección de datos personales. Todas las personas están expuestas a riesgos y abusos a raíz de la ausencia de una normativa robusta, más aún ante los nuevos desafíos que imponen las tecnologías.

La experiencia en Internet de las mujeres y minorías, como la comunidad LGBTI, es marcadamente distinta a la de los hombres. Las mujeres más activas -blogueras, periodistas y activistas en general- se exponen a un mayor riesgo de sufrir violencia de género en forma de agresiones, comentarios sexistas, amenazas y descalificativos, lo que provoca autocensura o cancelación de sus perfiles en redes. También los prejuicios de género desalientan el uso de las tecnologías por parte de las mujeres. Por estas razones, son necesarias políticas públicas que apunten a superar la brecha digital en términos de acceso y de uso.

Marco jurídico

Sobre la privacidad y la protección de los datos personales

La privacidad de las personas es un derecho humano protegido por normativas internacionales y nacionales. Algunos de los tratados que contemplan la protección de la vida privada son la Declaración Universal de Derechos Humanos, el cual señala que nadie será objeto de injerencias arbitrarias en su vida privada (art. 12, ONU, 1948). Lo mismo se recoge en el Pacto Internacional de Derechos Civiles y Políticos de Naciones Unidas (art. 17, inc. 1, ONU, 1966) y la Convención Americana sobre Derechos Humanos (art. 11, inc.

2, OEA, 1969). Todos estos tratados y convenciones han sido ratificados por Paraguay, lo que implica que pasan a ser parte de su sistema nacional legal.

El país cuenta con una fuerte protección constitucional a la intimidad y la inviolabilidad de la comunicación de las personas, así como el derecho a la autodeterminación informativa, principios directamente relacionados al derecho a la privacidad. Una serie de artículos de la Constitución Nacional (CN, Convención Nacional Constituyente, 1992) reconocen estas garantías: art. 33 sobre el derecho a la Intimidad, art. 36 de la inviolabilidad del patrimonio documental y de la comunicación privada, art. 23 de la prueba de la verdad y el art. 28 del derecho a informarse, en su párrafo final.

La protección de los datos personales es otra condición clave para el cumplimiento del derecho a la privacidad. Tiene reconocimiento constitucional en el artículo 135 de la CN, de la garantía del hábeas data: "Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad".

Los datos personales están regulados por la Ley Nº 1.682/01 (Congreso Nacional, 2001) "Que reglamenta la información de carácter privado" y su posterior modificación[1] por la Ley Nº 1.969 del año 2002 (Congreso Nacional, 2002) y por la Ley Nº 5.543/15. La ley 1682/01 asume que la acción de protección recae en la persona afectada, siendo más cercana a la doctrina norteamericana, que implica dejar el cumplimiento de la normativa a las partes involucradas y evitar la intervención del Estado, salvo en cuanto al rol que compete a los tribunales de justicia.

Sobre la promoción de la igualdad y la no discriminación hacia las mujeres

En lo que respecta a la promoción de la igualdad entre hombres y mujeres y la no discriminación, el Estado paraguayo ha ratificado la Convención para la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW por sus siglas en inglés) a través de la Ley Nº 1.215/86, y su Protocolo

1 Se puede acceder a un documento con la evolución de la ley, en el siguiente enlace: https://www.informconf.com.py/docs/Comparativo_ley_1682-01_y_modificatorias.pdf

Facultativo de la Convención para la Eliminación de Todas las Formas de Discriminación contra la Mujer Ley Nº 1.683/01.

Asimismo, ha adherido al Pacto Internacional de Derechos Económicos, Sociales y Culturales con la Ley N° 4/92, la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Belem do Pará) en la Ley N° 605/95, el Consenso de Montevideo y los Objetivos de Desarrollo Sustentable (ODS). Estos documentos internacionales tienen como objetivo la eliminación de todas las formas de discriminación contra la mujer o contra personas que son discriminadas por su orientación sexual o identidad de género.

El objetivo de estos principios es lograr la igualdad sustantiva en el goce de los derechos humanos y las libertades fundamentales. Como Estado Parte, Paraguay tiene la obligación jurídica de respetar, proteger, promover y cumplir con los principios y garantías contempladas en estos tratados.

La Constitución del país se refiere a estas garantías en los art. 46 "De la igualdad de las personas", art. 47 "De las garantías de igualdad" y el art. 48 "De la igualdad de derechos del hombre y la mujer".

Situación del derecho

Sobre la privacidad y la protección de los datos personales

El análisis de la legislación vigente[2] -y pese a las garantías constitucionales- revela que urge fortalecer estándares y prácticas de protección de datos personales. Todas las personas están expuestas a riesgos y abusos a raíz de la ausencia de una normativa robusta, más aún ante los nuevos desafíos que imponen las tecnologías.

La Ley Nº 1.682/01 (y sus modificaciones) tiene un enfoque meramente economicista, ya que regula casi exclusivamente los sistemas de información crediticia en las entidades bancarias y financieras, sin cubrir el resto de los aspectos sociales de la información personal. Consta de 12 artículos, de los cuales los artículos 5, 7, 9 y 10 regulan los informes crediticios.

2 Un análisis completo de la legislación sobre datos personales está disponible en la investigación de Acuña, Alonzo y Sequera (2017).

El ámbito de aplicación de la citada ley es el tratamiento de la información de carácter privado en general, cualquiera sea la forma en que este se lleve a cabo: "en archivos, registros, banco de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informe" (art. 1). Sin embargo, excluye específicamente a las bases de datos de su ámbito de aplicación, que es la forma más generalizada y masiva de almacenamiento de datos en la actualidad.

La redacción del artículo 1 genera confusión ya que por un lado afecta a los bancos de datos, pero excluye a las bases de datos y en ningún caso define qué es una u otra cosa. Según la Real Academia Española, un banco de datos es un "archivo de datos referidos a una determinada materia, que puede ser utilizado por diversos usuarios", mientras que base de datos es un "conjunto de datos organizado de tal modo que permita obtener con rapidez diversos tipos de información". Como puede observarse, y al no estar definidos uno u otro concepto, la Ley 1.682/01 prácticamente cae en una contradicción.

Si interpretamos que la citada ley excluye las bases de datos, se produce una contradicción con el concepto de autodeterminación informativa. Es decir, es necesario proveer al individuo de facultades que vayan más allá de la simple búsqueda del resarcimiento económico y otorgarle también instrumentos de actuación que permitan a los titulares controlar y determinar el destino u otros aspectos del tratamiento de sus datos personales, especialmente en registros públicos y privados en medios informáticos.

Excluir las bases de datos de la protección jurídica puede demostrar una falta de voluntad política en el momento de la redacción de la Ley 1.682/01 o un completo desconocimiento de las potencialidades de uso de dichas bases. Esta negligencia expone a las personas a ser individualizadas a través de sus datos personales, poniendo en riesgo la intimidad que es lo que se debería proteger. Esto ha provocado, entre otras cosas, la proliferación y el negocio de bases de datos de información de carácter personal y/o sensible, difundidas sin consentimiento y con fines comerciales. Además, se suman los riesgos a que se realicen cruzamientos a través de lo que se conoce como Big Data[3], aumentando las posibilidades de individualizar a las personas y discriminarlas.

Cabe agregar que la ley de referencia también carece de garantías ante la cesión y la comunicación de datos a terceros y que no contempla disposiciones

3 *Big Data* es la capacidad para aplicar análisis algorítmicos a los crecientes volúmenes de información que tanto empresas como gobiernos recolectan de las personas, lo que permite inferir, a través de correlaciones, información útil no contenida explícitamente en dichas bases de datos.

relativas a la transferencia internacional de datos. También se observa que no existen definiciones legales acerca de datos personales, tratamiento de datos y titular de datos.

Principios de protección

La Ley 1.682/01 no se ajusta a estándares garantistas como lo consagrados en los principios establecidos de protección de datos personales de la Directiva de la Unión Europea Nº 95/46 (Unión Europea, 1995) ni del nuevo reglamento general de protección de datos de la Unión Europea Nº 2.016/279, en especial falla en la figura de autodeterminación informativa.

Dicha ley tampoco incorpora efectivamente principios que regulan la protección de datos, como finalidad y limitación de finalidad, limitación en el plazo de conservación, integridad y confidencialidad, rendición de cuentas, seguridad, apertura y calidad del dato.

El principio de finalidad implica que la norma debería establecer los fines por los cuales los datos personales son recolectados. Es decir, el tratamiento de los datos personales debe ser cierto, adecuado, pertinente y no excesivo en relación al ámbito y finalidad para los que se hubieren obtenido. La Ley 1.682/01 no lo contempla.

Por otra parte, la misma ley considera lícita toda recolección, almacenamiento, procesamiento de datos personales para uso exclusivamente privado (art. 2) y solamente contempla su publicación cuando "se realice con fines científicos, estadísticos, de encuestas y sondeos de la opinión pública o de estudios de mercado, siempre que no individualicen a las personas o entidades investigadas" (art. 3). Es decir, limita el principio de finalidad considerando excepciones a los fines iniciales de la recolección.

Sobre la limitación en el plazo de conservación de los datos, la Ley 1.682/01 establece limitaciones en el tiempo necesario para los fines del tratamiento de los datos personales, pero solo limita su transmisión y divulgación según lo expresado en el art. 9 de la Ley Nº 5.543/15 y el art. 9 de la Ley Nº 1.969/02. No se establece nada sobre la eliminación de los datos, una vez transcurrido un tiempo determinado. Esta acción podrá realizarse a pedido del titular del dato.

La presente ley no contempla el principio de integridad y confidencialidad a través de la seguridad legal ante tratamiento de datos no autorizado o ilícito o contra la pérdida, destrucción o daño accidental. La única medida actual cae a cargo del afectado o titular del dato a través de la garantía constitucional.

Tanto el sector público como el privado, quiénes realizan tratamientos de datos deben estar sujetos a rendición de cuentas sobre medidas que toman para el manejo de los datos personales. A falta de un órgano especializado que garantice el cumplimiento de la rendición de cuentas, de transparencia y la aplicación de los estándares, el principio de rendición de cuentas se encuentra ausente en la legislación paraguaya.

Los principios de seguridad y apertura tampoco se han tenido en cuenta en la Ley 1.682/01. La información recolectada debería ser protegida frente a eventuales riesgos, como por ejemplo pérdida, sabotajes, destrucción, etc. Actualmente, el Plan Nacional de Ciberseguridad (CERT, SENATICS, 2016) incluye una serie de estándares para la protección de la infraestructura que almacena bases de datos para evitar estos problemas, pero desde un enfoque tecnológico: es decir, la protección solo se limita a la infraestructura y no se enfoca hacia las personas[4].

Por otra parte, en lo que respecta a la apertura, no existen políticas públicas sobre la apertura de información que guarde relación con el desarrollo, prácticas y normativas relacionadas al manejo de los datos personales.

El requisito de calidad del dato forma parte de los principios rectores de la Ley 1.682/01, pero nuevamente se limita a los informes crediticios, tales como situación patrimonial, solvencia económica y cumplimiento de obligaciones comerciales y financieras, obligando la actualización constante por parte de las empresas.

4 TEDIC, 8 de diciembre de 2016. *Aspectos positivos y negativos del Plan de Ciberseguridad en Paraguay,* Disponible en: https://www.tedic.org/aspecto-positivos-y-negativos-del-plan-de-ciberseguridad-en-paraguay/

Casos

La desprotección en las bases de datos personales

A raíz de la ausencia de una legislación robusta en materia de protección de datos personales, todas las personas están expuestas a abusos y riesgos por parte del sector privado y el sector público.

La investigación "¿Quién defiende tus datos?" (Sequera, 2017)[5], sobre los usos y prácticas de proveedoras de Internet (ISP por sus siglas en inglés), evidencia que las/os usuarias/os de sus servicios no tienen garantías adecuadas de protección de sus datos. Las empresas estudiadas –Tigo, Personal, Vox, Copaco, Claro y Chaco Comunicaciones– carecen de políticas de privacidad y de notificación a usuarias/os en caso que sus datos sean concedidos en el marco de investigaciones penales. Tampoco proveen informes de transparencia que detallen su gestión de información, y solo algunas se han posicionado en contra de la vigilancia. Las ISPs evaluadas no reconocen el rol central que juegan en la defensa de la intimidad de las personas.

Se destaca la preocupación manifestada por representantes de Tigo, Personal y Claro, que señalan su obligación de facilitar información de metadatos de llamadas telefónicas –conocidos como "cruce de llamadas"– por solicitud fiscal. Este mecanismo viola principios de la Constitución Nacional y tratados internacionales que exigen autorización judicial para acceder a registros de las comunicaciones de las personas. La investigación destaca que tanto Vox como Copaco no solamente retienen los datos/metadatos de las comunicaciones, sino que facilitan estas informaciones a los órganos de persecución penal violando el debido proceso.

En el sector público, la investigación "La protección de datos personales en bases de datos públicas"(Acuña, Alonzo Fulchi & Sequera, 2017) analiza los principios y prácticas aplicadas al manejo de los datos personales en nueve instituciones: la Secretaría Técnica de Planificación (STP), el Ministerio de Salud y Bienestar Social (MSPBS), el Centro Nacional de Computación (CNC), la Secretaría de Acción Social (SAS), el Ministerio de Industria y Comercio (MIC), la Dirección Nacional de Aduanas (DNA), la Subsecretaría de Estado de Tributación (SET), la Secretaría Nacional de la Vivienda y el Hábi-

5 Investigación que busca impulsar buenas prácticas entre las proveedoras de Internet para que protejan los derechos humanos y ofrezcan información clara sobre el uso de los datos de las personas que contratan sus servicios.

tat (Senavitat) y el Ministerio de Educación y Ciencias (MEC). Lo que surge de la investigación es que si bien hay indicios de la aplicación de buenas prácticas en algunos casos, el principal problema es la ausencia de una normativa robusta que aplique a todas las instituciones.

Otro problema que se evidencia, es que los responsables a cargo de las bases de datos tienen poca familiaridad con los estándares de protección de datos personales, ya sean regulaciones internas, nacionales o internacionales. Un principio que no se cumple es el de establecer un límite al almacenamiento de los datos personales. Casi todas las instituciones carecen de protocolos, mecanismos o normativas para la destrucción de dichos datos. Manifiestan diversas razones para no hacerlo. Sin embargo, se deben establecer criterios dependiendo de la naturaleza de las bases de datos.

Finalmente, existen dudas sobre la aplicación de principios de especificación de finalidad y limitación en el uso: se desconoce si los datos son utilizados solamente para los fines por los que son recolectados.

La serie "El retorno de los Pyrawebs"[6] resume varios de los problemas producto de la ausencia de un marco legal acorde a los desafíos de la evolución de las tecnologías y la digitalización de la información: el negocio creado a partir de la venta y compra de bases de datos personales; la perfección de los mecanismos de vigilancia del Estado; el manejo inescrupuloso de datos sensibles que resulta en hechos de discriminación; la proliferación de cámaras de vigilancia en espacios públicos; y el aumento de la recolección de datos biométricos.

La recolección de datos biométricos sin garantías de protección

Otro de los casos preocupantes, que agrava más la situación descrita en los párrafos anteriores es la recolección y almacenamiento de datos biométricos. En un contexto de normativa débil, los riesgos para las personas aumentan con dicha recolección, que implica la creación de nuevas bases de datos sin el debido control. La recolección de datos biométricos por parte de la Secretaría de Estado de Tributación (SET)[7] y el proyecto de Ley de "activación de telefonía móvil" son solo algunos ejemplos. Éste último, gracias al análisis y

6 El Surtidor, (s/f). Disponible en: https://elsurti.com/pyrawebs/

7 TEDIC, 25 de mayo de 2017. ¿Es legal la recolección de mis datos biométricos por parte de la SET? Disponible en: https://www.tedic.org/es-legal-la-recoleccion-de-mis-datos-biometricos-por-parte-de-la-set/

la difusión de los peligros de la normativa expuestos por TEDIC y el trabajo de incidencia de las proveedoras, fue vetado en su totalidad por el Poder Ejecutivo este año[8].

Los datos biométricos permiten la aplicación de métodos automatizados para reconocer de manera precisa a un individuo con base en las características físicas o de comportamiento. La tecnología usada en la biometría incluye el reconocimiento de huellas dactilares, huella palmar, facial, patrones de venas, iris, voces y otras exposiciones del cuerpo incluyendo el ADN y la secuencia de la pulsación de las teclas, entre otros.

La cuestión de la privacidad es fundamental para discutir sobre los alcances y los efectos de la biometría, ya que plantea un riesgo sustancial al derecho a la privacidad cuando no existen garantías mínimas de protección en el tratamiento de datos personales. El Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión de la ONU, Frank La Rue (Naciones Unidas, Consejo de Derechos Humanos, 2013) y el Alto Comisionado de Derechos Humanos, Navi Pillay[9], han expresado preocupación por las violaciones del derecho a la intimidad ante la falta de medidas de protección eficaces en la aplicación de las tecnologías biométricas.

La tecnología no es neutral, también discrimina

La ausencia de políticas para la reducción de la brecha digital de género en Paraguay, profundiza situaciones de desigualdad en la sociedad. En la investigación "Mejor educar que prohibir" (Galeano, 2016: 18), se expone la diferencia etaria de acceso a dispositivos móviles para acceder a Internet por parte de niños, niñas y adolescentes. Se evidencia que las mujeres acceden a un teléfono propio a partir de los 14 años de edad, mientras que los hombres a 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.

8 TEDIC, 28 de setiembre de 2017. *Acertada decisión del Poder Ejecutivo para la defensa de nuestra privacidad*. Disponible en: https://www.tedic.org/acertada-decision-del-poder-ejecutivo-para-la-defensa-de-nuestra-privacidad/

9 Centro de Noticias ONU, 12 julio de 2013. Disponible en: http://www.un.org/spanish/News/story.asp?NewsID=26945#.WgpJqlXibIU

Por otra parte, la violación del principio de neutralidad en la red[10] por parte de las ISPs genera otros problemas de brecha de género. Las ISPs a través de sus planes de "Facebook gratis" o "Whatsapp gratis", restringen el acceso a toda Internet al limitar la navegación a las condiciones del plan, particularmente en grupos vulnerables con escasos recursos. Algunas limitaciones podrían ser el acceso a información sobre temas de sexualidad y derechos sexuales y salud reproductiva. Esta información es necesaria para evitar embarazos no deseados de mujeres, niñas y adolescentes. En este último caso, son embarazos reconocidos como producto de violencia sexual ejercida por integrantes de la familia (abuso sexual incestuoso), conocidos, vecinos, o extraños[11].

Violencia de género en Internet

Según el informe de la World Web Foundation (2015), las mujeres más activas en Internet (blogueras, periodistas y activistas en general) se exponen a un mayor riesgo de sufrir violencia de género en forma de agresiones, comentarios sexistas, amenazas y descalificativos, lo que provoca autocensura o cancelación de sus perfiles en redes. El caso judicial de violencia de género en Internet contra la periodista Karen Ovando, en Paraguay, tuvo una sentencia positiva en la Cámara de Apelación[12]. Originalmente, la jueza GizelaPalumbo había ordenado a la organización TEDIC eliminar una publicación de su blog, en la que se analizaba la denuncia de la periodista. En dicha publicación se reprodujo el contenido publicado por la periodista, que mostraba una conversación de chat en la que los participantes masculinos bromeaban sobre su sexualidad y sobre la posibilidad de drogarla y violarla. La jueza, sin tomar en cuenta requisitos de idoneidad, necesidad y proporcionalidad, ni el interés público en el tema, ordenó retirar el contenido poniendo en riesgo la libertad de expresión de quienes trabajan para visibilizar la violencia en línea. Esta decisión fue revertida por la Cámara de Apelación en julio de este año y el contenido fue restituido.

10 La neutralidad de la red establece que no se puede discriminar ningún paquete de datos de ningún tipo, es decir, hacer diferencias durante el tráfico en su red entre un paquete de datos A y un paquete de datos B, ya sea por su origen o contenido. La ex Relatora Especial de la OEA para la Libertad de Expresión, Catalina Botero, afirma que la protección de la neutralidad es fundamental para garantizar la pluralidad y diversidad del flujo informativo. En este sentido, recuerda las palabras de la Corte Interamericana de Derechos Humanos (CIDH): "[E]l Estado no sólo [sic] debe minimizar las restricciones a la circulación de la información sino también equilibrar, en la mayor medida posible, la participación de las distintas corrientes en el debate público, impulsando el pluralismo informativo". En consecuencia, la equidad debe regir el flujo informativo. Disponible en: https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

11 Véase artículo sobre derechos sexuales y derechos reproductivos de este informe.

12 TEDIC, de 28 julio 2017. *Buena Noticia, el Tribunal de apelación revoca sentencia de primera Instancia sobre la censura a TEDIC por denunciar violencia de género.* Disponible en: https://www.tedic.org/buena-noticia-tribunal-revoca-sentencia-que-censuraba-a-tedic-por-denunciar-violencia-de-genero/

Las redes sociales, a través de sus algoritmos, afectan la privacidad y la libertad de expresión de usuarias. El informe del proyecto Online Censorship –que busca documentar los contenidos eliminados– ha demostrado que la gran mayoría de las denuncias por parte de usuarias/os desde noviembre de 2015 hasta marzo de 2016 estaban relacionadas con la desnudez, que subjetivamente se equiparaba con pornografía. Muchas de ellas incluían pezones femeninos[13], mientras que los masculinos pueden aparecer sin censuras en esas redes. Esta situación también afecta a usuarias en Paraguay, y se complejiza cuando grupos conservadores denuncian perfiles de activistas, provocando el bloqueo de sus perfiles como les ocurre sistemáticamente a las defensoras trans de la organización Panambí[14]. Según ellas, son criminalizadas por exponer su género en las redes sociales: cada cierto tiempo, varias de ellas sufren bloqueo de sus perfiles en Facebook porque son denunciados como perfiles falsos[15]. A ellas se les vuelve muy difícil recuperarlos porque se les obliga a presentar una identificación legal para recuperar sus cuentas. Hasta el presente año, el Estado paraguayo no reconoce legalmente el cambio de nombre y el género de las personas transexuales[16].

Por último, el Plan Nacional de Ciberseguridad es una política pública del gobierno paraguayo que busca hacer frente a los riesgos y desafíos que conlleva la tecnología. El Decreto Nº 7.052/17 contempla un análisis de los riesgos y otra de implementación de actividades. Uno de los aspectos preocupantes del plan es la visión de seguridad que está centrada en la infraestructura crítica o amenazas que se producen a través de la tecnología y no en la seguridad de las personas[17]. Sin embargo, el concepto de seguridad es mucho más amplio: por ejemplo, la seguridad de que una mujer acceda a Internet para encontrar información sobre cómo consumir pastillas anticonceptivas, o la posibilidad de consultar en foros de la web sobre cómo cuidar a su niño/a de una gripe.

Se deja casi al margen de la discusión el riesgo de la violación de derechos fundamentales de los ciudadanos a través del espionaje estatal y, en consecuencia, cómo se protegen las personas ante abusos del gobierno. También se desconoce la diversidad de experiencias de las personas, los peligros particu-

13 Online Censhorship, 21 de julio de 2016. Disponible en: https://onlinecensorship.org/es/news-and-analysis/la-moralidad-de-las-redes-sociales-de-como-facebook-censura-a-trump-y-la-sexualidad-femenina-por-igual

14 Es una organización que promueve y defiende los derechos de las personas trans en Paraguay buscando erradicar el estigma y la discriminación para la dignificación e inclusión social. Más información: http://www.panambi.org.py/

15 TEDIC, 5 de junio de 2017. *El derecho a aparición en Internet de la comunidad LGTBIQ.* Disponible en: https://www.tedic.org/el-derecho-a-aparicion-en-internet-de-la-comunidad-lgtbiq/

16 Véase artículo sobre derechos LGTBI de este informe.

17 TEDIC, 8 de diciembre de 2016. *Aspectos positivos y negativos del Plan de Ciberseguridad en Paraguay.* Disponible en: https://www.tedic.org/aspecto-positivos-y-negativos-del-plan-de-ciberseguridad-en-paraguay/

lares que ellas sufren. La violencia que viven las mujeres en Internet es marcadamente distinta a la que sufren los hombres. El cyber-acoso[18], doxing[19], y la sextorsión[20]son algunos ejemplos[21]. En el Plan tampoco se menciona la necesidad de avanzar en investigaciones de denuncia de espionaje estatal y violaciones al debido proceso. En estas graves transgresiones pueden esconderse situaciones de opresión a las mujeres, como de acoso, extorsión e intimidación. Como ejemplo, sigue pendiente una resolución al caso de espionaje militar a una periodista de ABC Color[22]. Además, es necesario someter a rendición de cuentas a las instituciones y las autoridades vinculadas a la compra de software de vigilancia[23].

Por último, debe incluirse un diagnóstico de los riesgos que implican las solicitudes de información de carácter personal de los usuarios que hace la Fiscalía a las proveedoras de Internet (ISP) sin orden judicial (Sequera, 2017). Todos estos hechos afectan las garantías constitucionales de la ciudadanía, y de manera muy particular la seguridad y el bienestar del 50% de la población.

Recomendaciones

Hacia una Ley orgánica de protección de datos personales

Es necesaria y urgente 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.

Esta nueva ley debe limitar el tratamiento de los datos personales en lo que respecta a: recolección, tiempo de almacenamiento, proporcionalidad, calidad del dato, ámbito de aplicación, transparencia, rendición de cuentas y otros principios establecidos por los estándares más altos de protección de datos personales con perspectiva de derechos humanos. También, la futura

18 El cyber-acoso es la práctica de atacar sistemática y sostenidamente a un individuo o grupo de personas causando algún tipo de daño sicológico o físico.

19 Doxing es la práctica de investigar y recopilar información de una persona o un grupo de personas con el objetivo de divulgar sus datos para violar su privacidad, intimidarlos o dañar su reputación.

20 La sextorsión se conoce a la práctica de extorsionar o amenazar a una persona con la posibilidad de divulgar sin su consentimiento fotografías o videos íntimos.

21 TEDIC, 9 mayo de 2017. *Buscando a las mujeres en el Plan Nacional de Ciberseguridad*. Disponible en: https://www.tedic.org/buscando-a-las-mujeres-en-el-plan-nacional-de-ciberseguridad/

22 TEDIC, 25 de agosto 2016. *Espionaje a periodista confirma que el Estado intercepta comunicaciones ilegalmente.* Disponible en: https://www.tedic.org/espionaje-a-periodista-confirma-que-el-estado-intercepta-comunicaciones-ilegalmente/

23 TEDIC, 20 de mayo 2016. 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/

Ley de Protección de Datos Personales deberá contemplar los avances tecnológicos: datos biométricos, algoritmos, big data, transferencias internacionales de datos, entre otros. A partir de estas conclusiones, se sugiere crear un órgano independiente como "ente rector" y responsable del control del tratamiento de datos, para analizar la finalidad del tratamiento y hacer las revisiones preventivas ante posibles errores o abusos que se puedan dar en el manejo de datos personales. Se agrega que es necesario auditar a los responsables de tratamientos de datos y elevar los estándares de protección, acorde a la Directiva de la UE Nº 95/46 y sus reglamentaciones.

Se enfatiza que la nueva ley no debe crear obstáculos a los avances de la Ley Nº 5.282/14 de acceso a la información pública. La misma debe contener dispositivos legales que aseguren el acceso a los datos personales cuando el interés público fuera mayor que la necesidad de sigilo, como la divulgación de salarios de los servidores públicos y otros casos.

Hacia una visión de seguridad digital para todos y todas

La desigualdad de género que el Estado se ha comprometido a superar, se debe también revertir en el entorno digital. El Plan Nacional de Ciberseguridad, siendo la política pública más importante en este aspecto, debe incorporar un enfoque centrado en las personas y sus experiencias, especialmente mujeres y minorías. Por ejemplo, en la parte del Plan que se menciona incluir la educación en TIC en la currícula educativa, la pregunta que surge es qué tipo de formación se inculcará para superar la desigualdad de género. La exclusión de las mujeres se da no solo en el acceso, sino en la creación de las tecnologías. Una respuesta a esta situación requiere un cambio en la configuración de referentes y en deconstruir los roles de género. Sin un abordaje consciente (de género) sobre estos temas, sin contemplar las ideas que los estudiantes internalizan sobre las tecnologías, se corre el peligro de reproducir los mismos mitos, estereotipos y dinámicas que sostienen la desigualdad entre hombres y mujeres en todos los ámbitos.

Además, cualquier cambio en la red está ligado a cambios fuera de ella. Problemas como la brecha digital de género son insalvables si otros aspectos de la sociedad no se modifican. Por ejemplo, las mujeres deben ocupar y deliberar sobre las políticas de desarrollo tecnológico y gobernanza en Internet.

Bibliografía

Acuña, Jazmín; Alonzo Fulchi, Luis; Sequera, Maricarmen (2017). *La protección de datos personales en bases de datos públicas. Un estudio exploratorio.* Asunción, TEDIC. Disponible en: https://www.tedic.org/wp-content/uploads/sites/4/2017/09/La-protecci%C3%B3n-de-Bases-de-Datos-en-Paraguay_Documento-Final.pdf

Galeano, José (Coord.) (2016). *Es mejor educar que prohibir.* Asunción: Global Infancia/ UNICEF / Enfoque Territorial. Disponible en: https://www.unicef.org/paraguay/spanish/esmejoreducarqueprohibir.pdf

Naciones Unidas, Consejo de Derechos Humanos (2013). *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. A/HRC/23/40. 17 de abril del 2013.* Disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/06/PDF/G1313306.pdf?OpenElement

Secretaría Nacional de Tecnologías de la Información y Comunicación (2016). *Plan Nacional de Ciberseguridad*. Disponible en: http://gestordocumental.senatics.gov.py/share/s/m2uDswEUTDmrDBY2NFttIg

Unión Europea (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016*. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

Sequera, Maricarmen (2017). *¿Quién defiende tus datos? Buscando la transparencia de los intermediarios de internet en Paraguay.* Asunción, TEDIC. Disponible en: https://www.tedic.org/wp-content/uploads/sites/4/2017/04/QuienDefiendeTusDatos_TEDIC-EFF.pdf

World Web Foundation (2015). *Global Report – October 2105. Women's Rights Online. Translating access into empowerment.* Disponible en: http://webfoundation.org/docs/2015/10/womens-rights-online21102015.pdf