DERECHOS HUMANOS PARAGUAY 2018

DANDO UN CORAZÓN AL HOMBRE DE HOJALATA: DERECHOS HUMANOS EN LAS POLÍTICAS DE INFRAESTRUCTURA DE INTERNET

DERECHOS DIGITALES

Uno de los personajes de *El maravilloso mundo de Oz*, de L. Frank Baum, era un hombre de hojalata cuyo mayor deseo era conseguir un corazón humano. ¿Y para qué? Para tener sensibilidad. Quería "sentir". Esta obra demuestra que no podemos tampoco nosotros permitirnos vivir sin corazón, sin sensibilidad, y que igualmente si en las políticas de Internet no se logra humanizar, es decir incluir perspectivas de derechos humanos en temas de algoritmos, inteligencia artificial, *datamining* (minería de datos), *blockchain* (cadena de bloques), no alcanzará humanizar las soluciones tecnológicas para un real cambio social y elevar la calidad de vida de todas las personas.

Maricarmen Sequera Buzarquis

TEDIC

INTRODUCCIÓN

El mundo se encuentra ante nuevas narrativas y desarrollo de nuevas perspectivas que respeten los derechos humanos a través del uso de la tecnología.

Paraguay debe ser consciente de estos avances para salvaguardar los derechos digitales de las personas en el entorno en línea de la vigilancia masiva, almacenamiento de datos sensibles como los datos biométricos, de exclusiones al acceso a Internet, así como violaciones a la neutralidad en la red y la implementación del voto electrónico sin tener en cuenta perspectivas integrales para una política pública inclusiva.

Aquí se expondrán las políticas gubernamentales, leyes y uso de tecnología que, sin perspectiva de derechos humanos, pueden socavar la seguridad cibernética y debilitar aún más nuestras democracias latinoamericanas.

MARCO JURÍDICO

Privacidad y datos personales

La Constitución Nacional reconoce y garantiza el derecho a la intimidad (art. 33). Adicionalmente, junto con la Constitución, la Convención Americana sobre Derechos Humanos ("Convención Americana"), obliga al Estado paraguayo a respetar y proteger derechos tales como derecho a la libertad de opinión y expresión (art. 13), derecho a la reunión (art. 15) y derecho a la honra y dignidad (art. 11). Por otra parte, se encuentran en el Pacto Internacional de Derechos Civiles y Políticos (PIDCP), los derechos a la privacidad y libertad de expresión (arts. 17 y 19). Estos derechos están estrechamente vinculados y "el derecho a la privacidad se entiende a menudo como un requisito esencial para la realización del derecho a la libertad de expresión"[1].

El artículo 11 de la Convención Americana protege a los individuos frente a "la injerencia arbitraria o abusiva en su vida privada, en su familia, en su domicilio o en su correspondencia" y reconoce que "toda persona tiene derecho a la protección de la ley contra tal interferencia o ataques". Del mismo modo, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP) protege a los individuos de "interferencias ilegales con su vida privada, su familia, su domi-

1 Mandato del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue, sobre las consecuencias de la vigilancia de las comunicaciones por los Estados en el ejercicio de los derechos humanos a la intimidad y a la libertad de opinión y expresión. Documento A/HRC/23/40, 17 de abril de 2013. Disponible en https://documents-dds ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf ?OpenElement.

cilio o su correspondencia, ataques ilegales a su honor y reputación". La Observación general 16 del Comité de Derechos Humanos sobre el artículo 17 del PIDCP (1998) señala que "la legislación pertinente debe especificar en detalle las circunstancias precisas en que tales interferencias pueden ser permitidas"[2] y "debe ser hecha solamente por la autoridad designada por la ley, y en cada caso particular"[3]. Además, la recolección arbitraria de información personal por parte del Estado constituye un acto altamente intrusivo que "viola los derechos a la privacidad y a la libertad de expresión y puede contradecir los principios de una sociedad democrática".[4]

También se encuentra vigente la Ley N.° 1682/01 "Que reglamenta la información de carácter privado" que regula ciertos aspectos del tratamiento de datos en nuestro país, pero no cumple con estándares internacionales mínimos de protección de datos personales[5]. En este sentido, el mejor ejemplo internacional es la regulación N.° 2016/679[6] de la Unión Europea que entró en vigencia el 25 de mayo de este año y otorga mayor control de las personas sobre sus datos personales para mitigar los abusos del sector privado y del estatal. Este es un ejemplo a seguir en la consolidación de una legislación que proteja efectivamente todos los derechos anteriormente enunciados.

Por Ley N.º 5994/17, Paraguay ratifica la Convención sobre la Ciberdelincuencia, y el Protocolo Adicional al Convenio sobre Ciberdelincuencia relativo a la Penalización de Actos de Índole Racista y Xenófoba cometidos por medio de Sistemas Informáticos, un marco normativo que busca la armonización de la persecución de los delitos cibernéticos de forma transfronteriza.

Es importante resaltar que la Ley N.º 4439/11 introduce los delitos informáticos en la legislación nacional. Sin embargo, no se contempla expresamente el concepto de ciberdelito ni delito informático, sino que se definen las distintas conductas delictivas en las que intervienen de alguna manera las nuevas tecnologías de la información y las comunicaciones. Se centra en la protección mediante el derecho penal de datos y sistemas informáticos, excluyendo a los

2 Comité de Derechos Humanos. Observación General 16 sobre el art. 17 Derecho a la Intimidad, Documento Hri/Gen/1/Rev . 7 At 162 (1988), párrafo 8.

3 Ídem.

4 Haut-commissariat aux droits de L'homme office of the High Commissioner for human rights palais des nations 1211 Geneva 10, Switzerland – 2017. Disponible en https://docplayer.es/79223927-Haut-commissariat-aux-droits-de-l-homme-office-of-the-high-commissioner-for-human-rights-palais-des-nations-1211-geneva-10-switzerland.html.

5 TEDIC (2017). La protección de datos personales en bases de datos públicas en Paraguay. Disponible en https://www.tedic.org/la-proteccion-de-datos-personales-en-bases-de-datos-publicas-en-paraguay/.

6 Parlamento Europeo y Consejo de la Unión Europea. Reglamento (UE) 2016/679 del 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES.

delitos cibernéticos en general. Se espera que con el Convenio se puedan profundizar elementos jurídicos ausentes o poco claros en la tipificación y la graduación de las sanciones en la legislación nacional.

Libertad de expresión y derecho al anonimato

Estos derechos se encuentran reconocidos en la Constitución Nacional en sus artículos (26 "Libertad de expresión" y 32 "De la libertad de reunión"). Asimismo son reconocidos y protegidos el discurso anónimo de las restricciones gubernamentales por la Convención Americana, artículos 11 y 13). Al respecto, menciona el Relator especial del derecho a la Libertad de Opinión y de Expresión de Naciones Unidas, que no se trata solamente de redactar "artículos de opinión" o de participar en "foros de debate", sino que también implica la capacidad de convocar movilizaciones sociales, protestas, y organizarse políticamente, entre otras"[7].

Los artículos 19(3) del PIDCP y 13(2) de la Convención Americana, respectivamente, prevén circunstancias limitadas en las que un Estado parte puede restringir el derecho a la libertad de expresión. De conformidad con el artículo 19(3), estas restricciones deben ser "previstas por la Ley" y necesarias para "el respeto de los derechos o la reputación de los demás" o "para la protección de la seguridad nacional o del orden público, la salud y la moral pública". Posteriormente, se debe aplicar el test de los principios "de necesidad y proporcionalidad" y evaluar y balancear las medidas tomadas para mitigar cualquier medida que pueda poner a los derechos en riesgo. De conformidad con el artículo 13(2) de la Convención Americana, la libertad de expresión no puede ser objeto de censura previa y las restricciones deben estar "expresamente establecidas por la Ley en la medida necesaria para garantizar", "el respeto de los derechos o la reputación de los demás" o "la seguridad nacional, el orden público, la salud o la moral públicas".

> Toda legislación o iniciativa que restrinja la libertad de expresión "debe ser accesible al público" y debe ser "formulada con suficiente precisión para permitir que un individuo regule su conducta en consecuencia". Dicha legislación "no debe conferir discrecionalidad absoluta para restringir libertad de expresión a los encargados de su ejecución". Además, cualquier restricción a la libertad de expresión "debe ajustarse a estrictos criterios de necesidad y proporcionalidad" (Comentario General 34). Por último, las medidas restrictivas "deben ser el instrumento menos intrusivo

7 Relator Especial de la CIDH para la Libertad de Expresión, y el Internet, 2013 (Relatoría de Derechos Humanos de la CIDH, 2013).

> entre aquellos que podrían lograr su función protectora; deben ser proporcionales al interés a ser protegido" (Comentario General 27)". David Kaye, Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión de Naciones Unidas[8].

La participación de las personas en el debate público sin revelar su identidad es una práctica habitual en las democracias modernas. La protección del discurso anónimo favorece la participación de las personas en el debate público ya que, al no revelar su identidad, puede evitar ser objeto de represalias injustas por el ejercicio de un derecho fundamental.

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 el acceso a los derechos a la información y a la libertad de expresión en la red. Por un lado, su incumplimiento termina favoreciendo a los actores más poderosos, como las empresas de tecnología[9], y limitando la variedad y amplitud de contenidos a los que acceden las personas que contratan el servicio de Internet. 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[10].

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 abierta. La actual regulación no se encuentra ampliada en un reglamento u otro instrumento legal distinto de la resolución.

En el informe titulado "Libertad de expresión e Internet"[11], 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 di-

8 Haut-commissariat aux droits de L'homme office of the High Commissioner for human rights palais des nations 1211 Geneva 10, Switzerland - 2017. Disponible en https://docplayer.es/79223927-Haut-commissariat-aux-droits-de-l-homme-office-of-the-high-commissioner-for-human-rights-palais-des-nations-1211-geneva-10-switzerland.html.

9 TEDIC (2016). Maricarmen Sequera. Los dueños de Internet. Artículo de opinión sobre las relaciones de poder de las empresas de tecnología y la comunicación en el mundo. Disponible en https://www.tedic.org/los-duenos-de-internet/

10 TEDIC (2018). Maricarmen Sequera. *¿Cuál es el estado de libertad de expresión en línea en Paraguay?* Disponible en https://www.tedic.org/el-estado-de-libertad-de-expresion-en-linea-en-paraguay/.

11 CIDH (2013). *Libertad de expresión e Internet.* Relatoría de la CIDH. Disponible en https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf.

versidad del flujo informativo. En este sentido, recuerda las palabras de la Corte Interamericana:

> [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.

El principio de la neutralidad de la red, debe considerarse como un pilar fundamental, y generar igualdad de condiciones para competir en el mercado. Porque en su defecto, afecta gravemente la competencia entre los servicios que se ofrecen gratis y los que no, incrementando el poder y valor de los primeros, en desmedro de los segundos, como es el caso de WhatsApp con Signal, por ejemplo y otras aplicaciones de contenidos.

Derecho al voto

El sufragio es un derecho, deber y función pública del elector, tal como lo expresa el artículo 118 de la Constitución Nacional.

El mismo constituye la base del régimen democrático y representativo. Se funda en el voto universal, libre, directo, igual y secreto; en el escrutinio público y fiscalizado, y en el sistema de representación proporcional. Asimismo, el artículo 4 del Código Electoral paraguayo, Ley N.º 834/96, expresamente determina las características del voto como uno de los principios fundamentales para el ejercicio de la ciudadanía.

> En el sistema actual basado en el papel, cualquier persona alfabetizada y con una mínima capacitación puede participar de la supervisión y el conteo de votos durante toda la jornada y el proceso electoral. En el caso de voto electrónico, la tecnología aparece como interfaz, entre el votante y el voto, entre el observador y los resultados, además de realizar de forma automatizada los conteos.
>
> La cantidad de elementos que podrían funcionar mal, escapa a cualquier capacidad humana de auditar dichos problemas, salvo claro, que la persona sea un ingeniero electrónico o informático y tenga acceso a los datos, dentro de cada aparato así como al código fuente del *software* que lo gestiona[12].

12 TEDIC (2018). *Voto electrónico, solucionismo electrónico.* Disponible en https://www.tedic.org/voto-electronico-solucionismo-electronico/.

SITUACIÓN DEL DERECHO

Censura política en Internet

El proyecto de ley "Que obliga a proveedores de aplicaciones y redes sociales a suspender y retirar publicaciones con carácter ofensivo o difamatorio" (Expediente D-1745454) presentado por el diputado nacional Edgar Ortiz, se suma a la lista de iniciativas legislativas que buscan regular Internet en forma regresiva. El proyecto busca regular los contenidos en Internet a través de la suspensión y retirada de publicaciones que el Estado considere ofensivas o difamatorias contra los representantes estatales y candidatos a cargos públicos. 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 proceso[13].

Sumado a lo anterior, la propuesta genera redundancia legislativa, en vista de 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 (arts. 150 al 156 del CP) y acciones civiles y administrativas, estas últimas sugeridas por la Corte Interamericana de Derechos Humanos[14].

> Las expresiones ofensivas, falsas u odiosas no pueden quedar impunes, pero existen mecanismos legales para perseguir hechos punibles, siempre y cuando medie una orden judicial. Además es inadmisible 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 terminan siendo 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[15].

13 TEDIC (2017). *Un proyecto de Censura Política*. Disponible en https://www.tedic.org/un-proyecto-de-censura-politica/.

14 CIDH (2004) Caso Ricardo Canese vs. Paraguay . Disponible en http://www.corteidh.or.cr/docs/casos/articulos/seriec_111_esp.pdf

15 TEDIC (2017) "Submission to study on social media, search, and freedom of expression". Contribuciones escritas para la presentación sobre libertad de expresión en la era digital en Paraguay. Disponible en https://www.ohchr.org/Documents/Issues/Opinion/ContentRegulation/TEDIC.pdf

Otro elemento a considerar es que el proyecto carece de 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 CIDH analizó este tema y realizó propuestas relativas a los intermediarios, en el Capítulo IV del informe 2013. Se advierte sobre los posibles peligros y/o abusos que los administradores de red, así como aplicaciones de contenidos pueden ejercer en Internet.

Por su parte, la Relatoría Especial de Naciones Unidas (ONU) para la Libertad de Expresión, en su informe (ONU, 2014) 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 solo 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.

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 una simple solicitud por parte de los políticos, provoca que el contenido deba 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[16].

Neutralidad de la red, un principio estructural de la red que garantiza libertad de expresión y acceso a Internet de calidad

El proyecto de ley "Que obliga a empresas de telefonía públicas y privadas a brindar el acceso gratuito y equitativo a sitios de Internet estatales con contenido educativo, que ofrecen recursos *online* a plataformas para postulaciones a becas o cursos", presentado por la senadora Lilian Samaniego, tiene por objetivo asegurar el ejercicio del derecho al acceso universal y equitativo a los servicios de telecomunicaciones, tecnologías de información y comunicación; cuenta con 6 artículos, acompañado de una extensa justificación para brindar acceso a los sitios estatales educativos para la formación y capacitación en general de todas las personas.

> Esta medida es solicitada como excepción al principio de neutralidad de la red a todas las proveedoras de Internet (ISPs) del país con los siguientes criterios: interés público y el carácter educativo, se parte de un análisis de mercado de los servicios que se busca implementar y que el servicio sea proveído a todos los dispositivos sin distinción alguna. Esta práctica de excepción a la neutralidad de la red se denomina *zero-rating* (tasa cero).
>
> El riesgo de solicitar este tipo de discriminaciones a ciertas aplicaciones de contenidos distorsiona la elección de los usuarios en Internet y provocan que la misma sea más cara, evitando que las ISPs inviertan en infraestructuras necesarias para proveer Internet de calidad para todas las personas. La alternativa a una Internet cara no es dar acceso gratuito a un subconjunto de aplicaciones con *zero-rating*. Las ISPs hacen cálculos estratégicos para absorber esos costos que luego incorporan en la suscripción de telefonía móvil. Esto provoca el encarecimiento general de Internet. No porque Paraguay sea un país con escasos recursos solo deba buscar soluciones menos ambiciosas para acceder a una Internet de calidad[17].

Este proyecto de ley del Congreso no describe las funcionalidades de las plataformas educativas; por tanto, se desconoce si las mismas tendrán solo texto o incluirán reproducciones de video, interacciones con videojuegos para una actividad educativa lúdica, videollamadas con los tutores, etc. Si se pretende incluir todo lo mejor que ofrece Internet, significará un alto costo a las ISPs que

16 TEDIC (2018). *¿Cuál es el estado de libertad de expresión en línea en Paraguay?* Disponible en https://www.tedic.org/el-estado-de-libertad-de-expresion-en-linea-en-paraguay/.

17 TEDIC (2018). Maricarmen Sequera. *¿Por qué ofrecer plataformas estatales con Zero Rating es una forma de precarizar Internet?*. Disponible en https://www.tedic.org/zero-rating-es-una-forma-de-precarizar-internet/.

afectará el ancho de banda de sus servicios a nivel nacional y, en consecuencia, al derecho al acceso a Internet de toda la población. Este tipo de medidas distorsiona la diversidad que ofrece Internet abierta, en lugar de hacer una inversión genuina en la calidad del servicio de Internet para todas las personas.

Tampoco se tiene previsto que para realizar una investigación se necesita no solamente acceso a las bibliografías que ofrece la plataforma, sino que se acceda a otra documentación que por razones de propiedad intelectual no se puedan incluir en el sistema.

Desplegar servicios discriminatorios no es la forma correcta de aumentar el acceso a Internet, ya que también aumentan los riesgos para los derechos humanos. En cambio, aquellos que buscan expandir el acceso a Internet deberían invertir o crear incentivos para invertir en infraestructura. De esta forma, nos aseguramos de que todas las personas puedan beneficiarse de una red de Internet libre y abierta, que puede actuar como un vehículo para el disfrute de los derechos humanos y un estímulo para la innovación y el desarrollo a nivel mundial; ayudando a alcanzar los Objetivos de Desarrollo Sostenible (ODS) de los Naciones Unidas[18].

Cibercrimen

Uno de los principales desafíos del sistema penal paraguayo en el siglo XXI es afrontar las conductas delictivas en la era digital. En una primera etapa se han realizado reformas al Código Penal para incluir sanciones especiales a los delitos vinculados a la tecnología (Ley 4439/11). Por otra parte, en el 2017, el Paraguay ratifica el Convenio de Ciberdelincuencia de Budapest.

Este último es considerado como un instrumento legal que regulariza los esfuerzos internacionales en la persecución de la conducta delictiva por medios digitales, pero a su vez contiene fallas de forma y fondo, a pesar de que a primera vista se observe como una propuesta que garantiza la protección de los derechos humanos[19]. Ha tenido muchas críticas a nivel internacional, acerca de su enfoque de cómo prevenir y luchar contra el delito cibernético de manera efectiva y actualizada. Uno de los cuestionamientos es la implementación de conservación de datos tráfico, ya que es considerado "espinoso" al momento

18 Metas 9 y 10 de los ODS. Disponible en https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/.

19 Maricarmen Sequera, Marlene Samaniego. (2018, junio). *Cibercrimen: desafíos de la armonización de la Convención de Budapest en el sistema penal paraguayo.* Disponible en https://www.tedic.org/wp-content/uploads/sites/4/2018/09/minuta_TEDIC.pdf.

de su aplicación porque da pie a interpretaciones de retenciones de metadatos de forma masiva por parte de las proveedoras de Internet, similar a la Ley *pyrawebs*[20], que, a su vez, puede reforzar el discurso de la necesidad de una Ley innecesaria y desproporcionada que pone en riesgo los derechos humanos.

Las revelaciones[21] sobre adquisición de *software* de vigilancia por parte del Estado paraguayo, causa serias preocupaciones. Este tipo de *software* no deberá utilizarse como excusa para la armonización del Convenio. Su uso en el país no está claramente autorizado por la legislación interna, ni mucho menos regulada a su forma de utilización y alcance. En algunos casos, las normas son tan imprecisas que dejan abierta la puerta para su uso y pueden requerir garantías adicionales a las establecidas en una mera interceptación de comunicaciones. La existencia de estas normas imprecisas inhibe una discusión pública en el Congreso sobre la necesidad de establecer normas y garantías adicionales.

Datos biométricos para el acceso al seguro social estatal (IPS)

Con el argumento de parar la corrupción en el retiro de medicamentos, estudios de imágenes y de laboratorio, el Consejo del Instituto de Previsión Social (IPS) aprobó en el año 2015 el registro biométrico de todos sus asegurados, desde los dos años de edad. En el año 2016, entró a regir la resolución del Consejo de Administración de IPS N.° 003-050/16, que obliga a los pacientes o sus autorizados a registrar sus huellas dactilares para el retiro de medicamentos oncológicos de alto costo, para que luego el registro se regularice para todos los servicios de IPS. La farmacia del Hospital Central –junto con el Centro de Atención al Usuario (CAU)– implementó este procedimiento obligatorio para el retiro de medicamentos, extendiéndose gradualmente a todos los asegurados de IPS.

Durante los primeros meses del año 2016 se registraron las huellas dactilares de 1.000 pacientes para el retiro en la farmacia externa. La meta final de ese año era alcanzar a los 7.000 asegurados titulares y 21.000 autorizados, precisó la Dra. Gladys Coronel, jefa del departamento de Farmacias[22].

La implementación del sistema biométrico del IPS no se encuentra regulada en la legislación nacional paraguaya. Si bien se reconoce en la Constitución Nacional el derecho de Intimidad (art. 33), en la práctica no existen suficientes me-

20 Campaña contra la retención de datos de tráfico en Paraguay. Disponible en https://pyrawebs.tedic.org/.

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

22 ABC Color, 3 de septiembre de 2016. Disponible en http://www.abc.com.py/edicion-impresa/locales/toman-huellas-dactilares-para-retirar-medicamentos-1514833.html

didas para garantizar el cumplimiento de este derecho, como se evidencia en el tratamiento de los datos personales en bases de datos públicas y privadas[23].

La Ley N.° 1682/01 que regula ciertos aspectos del tratamiento de datos en nuestro país dista de cumplir con estándares mínimos de protección de datos personales, como la autodeterminación del titular de los mismos. Además, no exige que el tratamiento de los datos se realice considerando la finalidad de la recolección, el tiempo de almacenamiento, legalidad, proporcionalidad, calidad, ámbito de aplicación, transparencia, rendición de cuentas, entre otros principios. Una gran ausencia en esta resolución administrativa son las sanciones en caso de abusos en el tratamiento de datos sensibles y bases de datos por parte de cualquier entidad pública o privada.

La recolección masiva de datos biométricos es innecesaria y desproporcionada. Las iniciativas de vigilancia en espacios públicos con *software* de reconocimiento facial, así como la recolección de huellas dactilares por parte de IPS, son medidas intrusivas y desproporcionadas porque recolectan datos sensibles de personas que circulan en espacios públicos y sobre la salud –tanto de personas enfermas como familiares– independientemente de si han sido o no sospechosas de conductas indebidas y sin ninguna garantía aparente. La recolección de datos sensibles debe buscar otras medidas menos intrusivas e indiscriminadas para prevenir la actividad fraudulenta.

Reconocimiento facial y cámaras de vigilancia en los espacios públicos

Durante el inicio del mes de julio de este año, autoridades de diversos organismos del sector público presentaron *in extenso* el nuevo conjunto de equipos y servicios tecnológicos del Sistema 911 de la Policía Nacional, para la implementación en la ciudad de Asunción y el Área Metropolitana. Los mismos se adquirieron mediante la licitación pública FSU N.° 2/2017 "Para el otorgamiento de subsidio a través del fondo de servicios universales para la expansión del sistema de atención y despacho de llamadas de emergencia 911 de la Policía Nacional para la ciudad de Asunción y área metropolitana" (Conatel, 2017).

Estos equipos fueron distribuidos en zonas estratégicas de la ciudad y las 100 cámaras se suman a un total de 800 ya existentes en toda el área metropolitana. Las cámaras de reconocimiento de placas fueron colocadas en peajes y rutas,

23 TEDIC (2017). *La protección de datos personales en bases de datos públicas en Paraguay.* Disponible en https://www.tedic.org/la-proteccion-de-datos-personales-en-bases-de-datos-publicas-en-paraguay/

mientras que las "novedosas" cámaras de reconocimiento facial se colocaron en puntos de alta concentración y circulación de personas, como la Terminal de Ómnibus de Asunción, el Aeropuerto Internacional "Silvio Pettirossi" y la sede del Congreso Nacional. Estas últimas ya poseen una base de datos de 50.000 personas y puede ser fácilmente ampliada, según el proveedor del Estado que se encargó de explicar el sistema[24].

El reconocimiento facial, así como el reconocimiento de la huella dactilar, huella palmar, patrones de venas, iris, voces y otras exposiciones del cuerpo, incluyendo ADN y la secuencia de pulsación del teclado, entre otros, son considerados datos biométricos. Su recolección y uso consiste en métodos automatizados que pueden reconocer de manera precisa a un individuo con base en las características físicas, biológicas o de comportamiento.

Para justificar la recolección de datos biométricos, que son datos sensibles[25] se debe analizar si no hay alguna alternativa que afecte en menor medida a los derechos de las personas y pueda alcanzar los objetivos que se persiguen. La medida de instalación de cámaras biométricas que busca prevenir cualquier tipo de ilícito en las calles de Asunción, refleja una desproporción en cuanto al fin perseguido, a la vez que deja de lado el principio de una intervención mínima a través del aparato punitivo del Estado, propio de lo que se denomina "derecho penal mínimo".

Falencias del "tecnosolucionismo": voto electrónico

A partir de muchas denuncias en las redes sociales sobre casos de posible fraude en las elecciones presidenciales en Paraguay[26], se planteó la discusión de recurrir al voto electrónico y así evitar las prácticas de manipulación electoral, mejorando el monitoreo y la velocidad de procesamientos de votos.

Durante el proceso electoral, la participación ciudadana no se limita en elegir la candidatura en la boleta: las personas también pueden supervisar y auditar el acto electoral: se supone que la elección es un acto público y transparente.

En el sistema actual basado en el papel, cualquier persona alfabetizada y con una mínima capacitación puede participar de la supervisión y el conteo de votos

24 Agencia IP, 5 de mayo de 2018. Disponible en https://www.ip.gov.py/ip/sistema-911-amplia-su-red-de-cobertura-con-9-torres-y-154-camaras-de-vigilancia-instaladas/.

25 Maricarmen Sequera, Luis Alonzo Fulchi & Eduardo Carrillo (2018). *La enajenación continua de nuestros derechos: Sistema de identidad: biometría y cámaras de vigilancia no regulada en Paraguay.* Disponible en https://www.tedic.org/wp-content/uploads/sites/4/2018/07/La-enajenaci%C3%B3n-continua-de-nuestros-derechos_TEDIC_2018.pdf.

26 ABC Color, 24 de abril de 2018. Disponible en http://www.abc.com.py/nacionales/tsje-debe-explicaciones-a-la-ciudadania-1696480.html.

durante toda la jornada y el proceso electoral. En el caso de voto electrónico, la tecnología aparece como interfaz, entre el votante y el voto, entre el observador y los resultados, además de realizar de forma automatizada los conteos.

El sistema democrático requiere que todos los pasos esenciales de la elección estén sometidos a la verificación por parte del público (observadores electorales y delegados partidarios). Implementar un sistema de voto electrónico supone complejizar y en cierta medida perder el control ciudadano del proceso electoral. Es decir, que los pasos esenciales de la gestión electoral y de la determinación del resultado deberían ser pasibles de ser comprobados por el ciudadano de manera confiable y sin conocimientos técnicos especiales.

La incorporación de una máquina o una computadora está fuera del alcance de entendimiento de cualquier persona, con lo cual la capacidad de control de los procesos implicados en una votación pasa a estar en manos de un conjunto muy pequeño de personas (los técnicos). Esto aumenta los riesgos y vuelve menos democrático al proceso como totalidad. Es decir, la complejidad técnica implica una imposibilidad de control ciudadano y relega el análisis a un sector reducido como los informáticos, sociedad civil y empresas.

El marco normativo paraguayo determina claramente que el voto es secreto, es decir, el acto de votar no es un "acto público". La libertad para elegir las autoridades está garantizada por ese secreto y, si no se cumple, el sistema fracasa en su esencia. Los sistemas de votación electrónicos actuales vulneran esta garantía del secreto en el voto, pilar del sistema.[27] Por ejemplo, los sistemas actuales de voto electrónico que están siendo utilizados en Brasil, Venezuela e India, mezclan el orden de votos emitidos, una vez cerrada la mesa. Sin embargo, existen posibilidades de poder reconstruir dicho orden con los conocimientos informáticos adecuados. En el caso del papel, esto es imposible.[28]

Es importante mencionar a modo de ejemplo que países como Finlandia, Austria, Dinamarca, Irlanda y Holanda utilizaron en algún momento el voto electrónico y lo abandonaron por no poder asegurar el secreto del voto, ni la fiabilidad de los resultados. En este marco, la misma Corte Constitucional de Alemania declaró inconstitucional y prohibió el uso del voto electrónico[29] y desde entonces se abandonó el voto electrónico en este país.

27 CONICET (2017). *Análisis de factibilidad de la implementación de la tecnología en diferentes aspectos y etapas del proceso electoral*. Argentina: CONICET.

28 TEDIC (2018). *Voto electrónico: solucionismo electrónico.* Disponible en https://www.tedic.org/voto-electronico-solucionismo-electronico/.

29 Fundación Vía Libre, 6 de marzo de 2009. Disponible en https://www.vialibre.org.ar/2009/03/06/alemania-urnas-electronicas-anticonstitucionales/.

CONCLUSIONES Y RECOMENDACIONES

→ Lograr el rechazo –por parte del Congreso Nacional– del proyecto de ley de censura política 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.

→ Realizar una revisión integral de la propuesta de Ley de *zero-rating* para la educación. Esto, porque no se deben usar servicios especializados para eludir las reglas de una Internet abierta, o para ofrecer "algo" denominado servicios especializados como las plataformas educativas del sector público o privado, que básicamente es un reemplazo para el servicio de Internet de calidad. Esta discriminación que, a primera vista parece ser económica para el usuario final, sin embargo genera degradación de la calidad del servicio y pone en riego derechos, como libertad de expresión y el acceso a la información.

→ Aplicar el Convenio de Budapest, teniendo en cuenta la diversidad cultural, política y económica de los países. Esto, para disminuir las barreras de seguridad nacional, entrando en conflicto con el interés público y los derechos humanos. Es necesario realizar salvedades para no ceder jurisdicción y privacidad de forma desproporcionada. Se debería priorizar el conocimiento sobre el contenido y alcance del mismo. Debe darse un debate amplio, calmo y sereno entre todos los sectores de la sociedad con plena participación ciudadana a nivel nacional y regional, para conjuntamente elaborar una armonización eficaz y que respete los derechos humanos.

→ Fortalecer a las instituciones y operadores de justicia para una mejor interpretación de las leyes nacionales e internacionales en el ámbito penal sobre vigilancia de las comunicaciones, dado el avance de las técnicas y tecnologías de vigilancia. Para que los jueces del Poder Judicial realicen un análisis de proporcionalidad de Ley o sobre el uso de *software* malicioso como FinFisher, o cualquier otra forma de interceptación de las comunicaciones (incluyendo los metadatos), deberán estar capacitados para conocer y justificar su uso, y así evitar negligencias o abusos por parte de otras instituciones como la Secretaria Nacional Antidrogas (Senad), Policía Nacional o Ministerio Público.

→ Transparentar el *software* de datos biométricos, tanto en su uso, como en su alcance. Agregando la información necesaria para conocer la tecnología y los

mecanismos utilizados para la vigilancia biométrica, debido a la amenaza creciente contra la privacidad.

→ Promover la creación de una Ley integral de datos personales en Paraguay. El país carece de un marco jurídico suficiente que permita garantizar un adecuado tratamiento de datos biométricos recolectados, tanto por parte del Estado como el sector privado. En la actual legislación, los datos de salud aún se consideran particularmente sensibles y vulnerables en relación con los derechos fundamentales o la privacidad, sin embargo merecen una protección específica.

→ Crear y promulgar una Ley de protección de datos personales que tenga en cuenta no solamente la defensa basada en los derechos humanos, sino también la creación y defensa de modelos económicos más inclusivos y confiables en el entorno en línea.

→ Concentrar esfuerzos (del Gobierno y las autoridades) en implementar políticas basadas en evidencia. Deben analizar previamente el contexto y las medidas a tener en cuenta para la persecución de delitos, y evitar que el impacto no sea solamente beneficiar a la industria de la vigilancia, sino principalmente mejorar la calidad de vida de las personas.

→ Desestimar la idea de implementación del voto electrónico. No puede considerarse un mecanismo que garantice la calidad democrática del sistema electoral. Además, es posible y razonable aplicar ciertas tecnologías digitales en el contexto de los sistemas electorales fuera del acto específico del voto, como por ejemplo el "TREP" (transmisión rápido de resultados preliminares). Este es un buen ejemplo de digitalización pero que aún necesita más ajustes).

→ Modificar el Código Electoral vigente para garantizar que los mecanismos se adecuen a la realidad actual, sobre todo para tratar de bloquear los mecanismos de manipulación electoral que se vienen dando desde la restauración democrática.

BIBLIOGRAFÍA

Asamblea Constituyente (1992). *Constitución Nacional de la República del Paraguay.* Disponible en http://www.bacn.gov.py/constitucion-nacional-de-la-republica-del-paraguay.php.

CONATEL (2017). CIRCULAR 1 - Licitacion-2-2017.pdf. Disponible en ttps://www.conatel.gov.py/images/iprincipal/2017/Noviembre/Licitaci%C3%B3n%20Publica%20FSU%20N%C2%B02/CIRCULAR%201%20-%20Licitacion-2-2017.PDF.

Congreso Nacional (2001). Ley N.° 1682/01 "Que Reglamenta la información de carácter privado, 1682/01". Disponible en http://www.bacn.gov.py/ampliar-leyes-paraguayas.php?id=1760.

Congreso Nacional (2011). Ley 4439 que modifica y amplia varios artículos de la Ley N.° 1160/97 "Código Penal". Disponible en http://www.bacn.gov.py/archivos/3777/20150817113434.pdf.

Congreso Nacional (2017). Expediente: D-1745454 Que obliga a proveedores de aplicaciones y redes sociales a suspender y retirar publicaciones con carácter ofensivos o difamatorio. Disponible en http://silpy.congreso.gov.py/expediente/110839.

Congreso Nacional (2018). Expediente: S-187987 "Que obliga a empresas de telefonía públicas y privadas a brindar el acceso gratuito y equitativo a sitios de internet estatales con contenido educativo, que ofrecen recursos *online* a plataformas para postulaciones a becas o cursos". Disponible en http://silpy.congreso.gov.py/expediente/113555.

Maricarmen Sequera, Luis Alonzo Fulchi, & Eduardo Carrillo (2018). *La enajenación continua de nuestros derechos. Sistema de identidad: biometría y cámaras de vigilancia no regulada en Paraguay*. Disponible en https://www.tedic.org/wp-content/uploads/sites/4/2018/07/La-enajenaci%C3%B3n-continua-de-nuestros-derechos_TEDIC_2018.pdf.

Maricarmen Sequera, Marlene Samaniego (2018). *Cibercrimen: desafíos de la armonización de la Convención de Budapest en el sistema penal paraguayo.* Disponible en https://www.tedic.org/wp-content/uploads/sites/4/2018/09/minuta_TEDIC.pdf.

ONU (2013). *Report of the Special Rapporteur to the Human Rights Council on the implications of States surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression.* A/HRC/23/40. Disponible en https://documents-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement.

ONU. (2014). ACNUDH | RE sobre libertad de opinión y de expresión. Disponible en https://www.ohchr.org/SP/Issues/FreedomOpinion/Pages/OpinionIndex.aspx.

Relatoría de Derechos Humanos de la CIDH. (2013). Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos Humanos. Catalina Botero (p. 93). OEA. Disponible en https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf.

Rolón Luna, J., & Sequera Buzarquis, M. (2016, marzo). *Vigilancia Estatal de las comunicaciones y derechos fundamentales en Paraguay.* Disponible en https://www.tedic.org/wp-content/uploads/sites/4/2016/05/Paraguay-ES.pdf.

TEDIC. (2017). *La protección de datos personales en bases de datos públicas en Paraguay.* Disponible en https://www.tedic.org/la-proteccion-de-datos-personales-en-bases-de-datos-publicas-en-paraguay/.