DERECHOS HUMANOS PARAGUAY 2020

CODEHUPY
Coordinadora de Derechos Humanos del Paraguay

DERECHOS HUMANOS PARAGUAY 2020

CODEHUPY
Coordinadora de Derechos Humanos del Paraguay

ORGANIZACIONES PARTICIPANTES

- Aireana - Grupo por los derechos de las lesbianas
- Asociación de Ciencia Política del Paraguay (ACIPP)
- Asociación Latinoamericana de Medicina Social y Salud Colectiva (Alames)
- BASE - Investigaciones Sociales (BASE-IS)
- Centro de Documentación y Estudios (CDE)
- Centro de Investigación Multidisciplinaria para el Desarrollo (CIMDE)
- Centro de Investigación, Desarrollo e Innovación de la Facultad de Arquitectura, Diseño y Artes de la UNA
- Confederación de la Clase Trabajadora (CCT)
- Coordinación de Mujeres del Paraguay (CMP)
- Coordinadora de Derechos Humanos del Paraguay (Codehupy)
- Coordinadora por los Derechos de la Infancia y la Adolescencia (CDIA)
- Decidamos, Campaña por la Expresión Ciudadana
- Enfoque Territorial
- Fábrica Social
- Fundación Yvy Marãe'ỹ
- Gente, Ambiente y Territorio (GAT)
- Hábitat para la Humanidad - Paraguay
- Heñói - Centro de Estudios y Promoción de la Democracia, los Derechos Humanos y la Sostenibilidad Socio-ambiental
- Iniciativa Amotocodie
- Kuña Róga
- Movimiento por el Derecho a la Salud "María Rivarola"
- Organizaciones de la Sociedad Civil, integrantes de la Comisión Nacional por los Derechos de las Personas con Discapacidad (Conadis)
- Panambi - Asociación de Travestis, Transexuales y Transgéneros del Paraguay
- Plataforma Social de Derechos Humanos, Memoria y Democracia
- Red Contra Toda Forma de Discriminación (RCTD)
- Semillas para la Democracia
- Servicio Paz y Justicia - Paraguay (Serpaj-Py)
- Unidas en la Esperanza (UNES)
- Tape'a para el desarrollo social sostenible
- Techo Paraguay
- Tecnología y Comunidad (Tedic)
- Tierraviva a los Pueblos Indígenas del Chaco
- Unidas en la Esperanza (UNES)

DERECHOS DIGITALES EN MODO COVID-19

Esta es la quinta ocasión consecutiva en que los derechos digitales integran el informe anual de la Codehupy y, a lo largo de estos años, se observa un salto importante en el acceso de las personas a Internet en Paraguay. Por lo tanto, se evidencia la importancia de fortalecer los derechos humanos en el entorno en línea. Desde aquel tiempo, y en especial en el periodo del presente informe, se ha observado un gran recrudecimiento de las normativas de vigilancia estatal de las comunicaciones, de las violaciones de libertad de expresión en línea, de la violencia digital de género, así como abusos en el tratamiento de datos personales. Las políticas públicas sobre tecnología e inclusión digital deben apuntar a mejorar la calidad de vida y la integridad de las personas en entornos digitales, en vez de avasallar y violentar derechos.

PALABRAS CLAVES: privacidad, datos personales, género en Internet, libertad de expresión, vigilancia de las comunicaciones.

Maricarmen Sequera Buzarquis y Paloma Lara Castro Escobar

TEDIC

BALANCE DE LOS 25 AÑOS

LOS DERECHOS HUMANOS TAMBIÉN EXISTEN EN INTERNET

Los derechos digitales nacen a partir de la necesidad de contar con una respuesta jurídica precisa para toda actividad relacionada con los servicios de la sociedad de la información y de la comunicación. Si bien son los derechos humanos propiamente dichos, que surgen como resultado del reconocimiento de los derechos fundamentales en la red de redes, actualmente cuenta con su propia regulación, lenguaje y elementos tecnológicos. Este elemento tecnológico es transversal, sobre todo Internet, que está atravesando en nuestras vidas, al igual que está ocurriendo en el derecho.

La capacidad de compartir información y comunicarse libremente a través de Internet es la piedra angular para la realización de los derechos humanos consagrados en la Declaración Universal de Derechos Humanos (1948), el Pacto Internacional de Derechos Económicos, Sociales y Culturales (1976), el Pacto Internacional de Derechos Civiles y Políticos (1976) y la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW, 1980).

Una de las primeras declaraciones sobre derechos digitales la hizo Robert B. Gelman, quien en 1997 difundió una propuesta de Declaración de los Derechos Humanos en el Ciberespacio, delineada sobre la base de la Declaración Universal de los Derechos Humanos de 1948. En la Declaración de Itacuruçá (2000) se consagra por primera vez el derecho al acceso democrático a la sociedad del conocimiento. También se encuentra la Declaración de Independencia del Ciberespacio de John Perry Barlow, de 1996, donde se entiende a Internet como un camino abierto para la mejora de la condición humana y de la sociedad. La Declaración de Florianópolis (2000) recoge la aspiración de los países latinoamericanos de integrarse en la sociedad de la información. Entre estos esfuerzos se destaca la Declaración Conjunta sobre Libertad de Expresión e Internet, del año 2011, por las diversas relatorías para la libertad de expresión de la Organización de las Naciones Unidas (ONU). Desde entonces, los organismos internacionales y los Estados han puesto su interés en cubrir estos temas desde un enfoque integral para el desarrollo de las sociedades.

En Paraguay surge esta discusión e interés con la ola global de las reformas de propiedad intelectual en Internet y la descentralización de servicio de Internet exclusivamente estatal desde el 2007 hasta el inicio del 2010, que más tarde dio lugar al nacimiento de la Asociación Tedic, que trabaja en estos temas desde hace 8 años.

AVANCES Y RETROCESOS

En este último quinquenio se observa un importante avance en materia de derechos digitales en la agenda del Estado, sector privado, organizaciones de sociedad civil, academia y comunidades técnicas en Paraguay. Y esto se debe a que en los recientes años han aumentado el acceso a Internet y el uso de las tecnologías en general en América Latina. Es decir, la penetración de Internet se incrementó en todos los países y quintiles entre el 2011 y el 2015. Sin embargo, en Paraguay, el acceso a Internet sigue sumamente desigual entre los hogares más ricos y los más pobres. La diferencia es de 20 veces superior del quintil más rico con relación al quintil más pobre. La brecha de conexión entre zona urbana y rural es de 20 puntos porcentuales. Además, menos del 50% de la población cuenta con acceso a Internet y la velocidad promedio es de 11,5 Mbps. De esta forma, el país se ubica en uno de los últimos lugares en América del Sur[1].

A medida que más personas acceden a este espacio digital, sin una política pública integral en tecnología basada en la vida de las personas, muchas de ellas quedarán excluidas. Al igual que el proceso de globalización con el que ha estado estrechamente entrelazada, la expansión del acceso a Internet se produce con resultados desiguales y a menudo exacerba las desigualdades socioeconómicas. Esto se ha evidenciado en tiempos de emergencias de la salud, con políticas públicas "parches" que obligaron a los servicios públicos, la educación y el trabajo en general se trasladen abruptamente a Internet. Esto generó una gran brecha digital y de género, excluyendo a personas que no cuentan con acceso de calidad a Internet, habilidades y destrezas digitales[2].

Asimismo, entre los aspectos más alarmantes de los últimos años se han notado un recrudecimiento de las normativas de vigilancia estatal y un aumento de recursos a las instituciones del sistema penal y vigilancia Estatal, sin un marco jurídico legal que permita y limite la utilización de tecnología de alta intromisión a la vida privada de las personas.

HITOS RELEVANTES DE LOS DERECHOS DIGITALES EN PARAGUAY

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (MITIC). En el 2018 se creó esta institución, cuyo fin es diseñar e implementar políticas públicas que promuevan y faciliten la conectividad, la inclusión, la innovación tecnológica y la economía digital. Antes de llegar a ser Ministerio, tuvo varias modificaciones administrativas estructurales.

1 Maricarmen Sequera, 27 de abril de 2020, "La educación virtual y la infraestructura de Internet en Paraguay". *Blog de Tedic*, https://www.tedic.org/la-educacion-virtual-y-la-infraestructura-de-internet-en-paraguay/.

2 Ibíd.

Este cambio significó la creación de una agenda digital muy ambiciosa, que se encuentra en pleno desarrollo y que comprende políticas de inclusión digital con perspectiva de derechos humanos. El desafío está en desarrollar metodologías de participación de todos los sectores, en el marco de la transparencia, la rendición de cuentas, la participación ciudadana y con una evaluación previa del posible impacto de las políticas en los derechos humanos.

LEY N.º 5777/2016 "DE PROTECCIÓN INTEGRAL A LAS MUJERES CONTRA TODA FORMA DE VIOLENCIA". Esta normativa[3] es la primera que incluye a la *violencia telemática* como una forma de violencia que ocurre en Internet. Este avance legal significó ampliar la aplicación de la ley en espacios digitales. Sin embargo, el desafío está en crear mecanismos efectivos para su aplicación.

RECHAZO DE LA LEY "PYRAWEBS" Y OTRAS SIMILARES. En el 2015 se logró el rechazo de un proyecto de ley denominado "Conservación obligatoria de datos de tráfico", coloquialmente conocido como Ley "Pyrawebs". Esta normativa pretendía obligar a proveedoras de Internet a retener los metadatos de tráfico durante 12 meses, poniendo en riesgo la privacidad de todas las personas por ser una medida desproporcionada y masiva de vigilancia de las comunicaciones[4]. La iniciativa "anti-Pyrawebs" fue la primera campaña ciudadana enteramente digital sobre derechos digitales, que tuvo como consecuencia el rechazo absoluto y archivo del proyecto de ley[5]. Además, logró concientizar un tema muy complejo, como es la tecnología en un contexto con baja conectividad a nivel nacional[6]. Tomando esta campaña como impulso, se han logrado frenar otras normativas parecidas[7] y se ha alertado a

3 Ley N.º 5777, del 27 de diciembre de 2016, de protección integral a las mujeres contra toda forma de violencia, *Biblioteca y Archivo Central del Congreso de la Nación*, https://www.bacn.gov.py/leyes-paraguayas/8356/ley-n-5777--de-proteccin-integral-a-las-mujeres-contra-toda-forma-de-violencia.

4 "La Retención de Datos de Tráfico en Paraguay Es Espionaje Masivo e Inconstitucional", *Electronic Frontier Foundation*, acceso el 8 de marzo de 2016, https://www.eff.org/es/deeplinks/2014/11/la-retencion-de-datos-de-trafico-en-paraguay-es-espionaje-masivo-e.

5 Javier Pallero, "Breaking news: 'Pyrawebs' rejected for good", *Access Now*, 4 de junio de 2015, acceso el 10 de octubre de 2020, https://www.accessnow.org/breaking-news-internet-data-retention-bill-pyrawebs-rejected-for-good-espan/.

6 Maricarmen Sequera, "La educación virtual y la infraestructura de Internet en Paraguay".

7 Algunos casos fueron:
1. Ley N.º 5883/2017, "Que regula la activación del servicio de telefonía móvil", presentada en el 2017. "Acertada decisión de vetar el proyecto de ley de registro de huellas dactilares para acceder a servicios de Internet", *Blog de Tedic*, 28 de septiembre de 2017, https://www.tedic.org/acertada-decision-del-poder-ejecutivo-para-la-defensa-de-nuestra-privacidad/.
2. Proyecto de ley "Que obliga a proveedores de aplicaciones y redes sociales a suspender y retirar publicaciones con carácter ofensivo o difamatorio, presentado por el diputado Edgar Ortiz en el 2017. "Se archiva el proyecto de ley de Censura política en Internet", *Blog de Tedic*, 11 de octubre de 2017, https://www.tedic.org/un-proyecto-de-censura-politica/.
3. Proyecto de ley "Que sanciona el incumplimiento de las medidas dispuestas ante alertas epidemiológicas y en estado de emergencia sanitaria declarada", presentado el 18 de marzo de 2020 y retirado poco tiempo después, el 1 de abril. "El Congreso paraguayo retira el proyecto de ley sobre desinformación en tiempos de emergencia", *Blog de Tedic*, 3 de abril de 2020, https://www.tedic.org/el-congreso-paraguayo-retira-el-proyecto-de-ley-sobre-desinformacion-en-tiempos-de-emergencia/.
4. Rechazo de una acción de amparo constitucional que buscaba censurar una publicación de un activista en Twitter. "El Poder Judicial aboga por la defensa de la libertad de expresión", *Blog de Tedic*, 16 de junio de 2016, https://www.tedic.org/una-victoria-en-favor-de-nuestra-libertad-de-expresion-en-internet/.

la ciudadanía sobre acciones del Estado que conllevan un alto riesgo para el ejercicio pleno de derechos en los espacios digitales.

SISTEMA NACIONAL DE INTELIGENCIA (SINAI). Creado en el 2014[8], está compuesto por varias instituciones del Estado orientadas a trabajos de inteligencia. El Sinai, la Secretaría Nacional Antidrogas (Senad), las Fuerzas Armadas y el Ministerio del Interior no cuentan con la obligación de publicar informes sobre las actividades de vigilancia de las comunicaciones, por lo que operan con total autonomía, poca supervisión efectiva o, dicho de otra forma, con total impunidad.

VOTO ELECTRÓNICO. La implementación del voto electrónico como solución tecnológica ante los diversos tipos de irregularidades que ocurren en las elecciones nacionales ha sido otro importante hito. Esta "solución" tiene varios riesgos, expuestos en el informe anterior[9]. Sin embargo, el Tribunal Superior de Justicia Electoral (TSJE) ha ignorado y ha realizado la licitación de alquiler de las máquinas de votación, cuya implementación está paralizada por la emergencia sanitaria actual[10].

SISTEMAS DE VIGILANCIA DE LAS COMUNICACIONES

Como resultado de la falta de transparencia de las políticas y prácticas de la vigilancia en Paraguay, no queda claro qué tipo de capacidades posee el país. Sin embargo, en los últimos años han aparecido varios informes que dan cuenta de la existencia de sistemas de vigilancia de las comunicaciones en la órbita estatal, y esto difiere sustancialmente de lo que está indicado en la ley. Como ejemplos de esto se pueden citar: la adquisición del *malware* llamado FinFisher[11], las conversaciones para la adquisición del *malware* de Hackingteam[12], el uso de cámaras de reconocimiento facial[13], así como la adquisición de drones para vigilancia en espacios públicos[14].

8 Ley N.º 5241, de 20 de agosto de 2014, que crea el Sistema Nacional de Inteligencia, *Biblioteca y Archivo Central del Congreso de la Nación*, http://www.bacn.gov.py/NDYyMA==&ley-n-5241.

9 Maricarmen Sequera y Paloma Lara Castro, "¿Quién vigila al vigilante?", en *Derechos Humanos en Paraguay 2019* (Asunción: Codehupy, 2019), 365-390.

10 "Máquinas de votación podrían no salir de Argentina por Covid-19", *Última Hora*, 23 de marzo de 2020, acceso el 14 de abril de 2020, https://www.ultimahora.com/maquinas-votacion-podrian-no-salir-argentina-covid-19-n2876321.html.

11 Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto y Sarah Mckune, "Pay No Attention to the Server Behind the Proxy. Mapping FinFisher's Continuing Proliferation", en *The Citizen Lab*, 15 de octubre de 2015, acceso el 27 de septiembre de 2020, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

12 "The Hackingteam Archives", *WikiLeaks*, 8 de julio de 2015, acceso el 3 de abril de 2017, https://wikileaks.org/hackingteam/emails/emailid/4132.

13 "Reconocimiento facial: nueva estrategia para combatir la delincuencia", *ABC Color*, 11 de julio de 2019, acceso el 11 de julio de 2019, https://www.abc.com.py/nacionales/2019/07/11/reconocimiento-facial-nueva-estrategia-para-combatir-la-delincuencia.

14 Paloma Lara Castro, "Uso de drones: ¿combaten la pandemia o refuerzan el control ciudadano?", *Blog de Tedic*, 22 de abril de 2020, https://www.tedic.org/uso-de-drones-covid19/.

En el marco de las actividades de vigilancia, en 2016, Paraguay aceptó las recomendaciones del Examen Periódico Universal (EPU)[15]. A pesar de esto, recientemente se realizó una solicitud de acceso a información pública al Ministerio de Relaciones Exteriores de Paraguay, que fue respondida de la siguiente forma: "[...] No se cuenta aún con el seguimiento correspondiente por parte de las instituciones competentes [...]"[16].

El Ministerio del Interior[17] y la Senad[18] han respondido a la solicitud de información pública compartiendo la normativa que les permite monitorear las comunicaciones. Sin embargo, se considera que no son suficientes para aclarar las adquisiciones y el uso de *hardware* y *software* específicos para la vigilancia de las comunicaciones que se describen en este documento. La regulación compartida por estas instituciones solo alude a la interceptación telefónica. En cuanto a la solicitud de información sobre los mecanismos de rendición de cuentas acerca de la adquisición de *software* de vigilancia, solo se refieren a cuestiones administrativas relacionadas con salarios, lista de funcionarios, adquisiciones de bienes, etc., pero no brindan la información sobre la consulta realizada en el Portal de Acceso a la Información Pública.[19]

Ante la falta de un monitoreo y control de posibles abusos por parte de estas instituciones del Estado, se han realizado litigios estratégicos para solicitar información sobre la adquisición, implementación y uso de algunas de estas

15 Los derechos implicados sobre las recomendaciones son: libertad y seguridad de la persona, no violencia, derechos civiles y políticos y alcance de las obligaciones internacionales. Las instituciones implicadas en el cumplimiento y seguimiento de estas recomendaciones son: Comisión Nacional de Telecomunicaciones, Ministerio del Interior, Secretaría Nacional de Tecnologías de la Información y Comunicación (actualmente Ministerio de Tecnologías de la Información y Comunicación) y Ministerio de Defensa Nacional. El Objetivo de Desarrollo Sostenible (ODS) afectado: 16. Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y construir a todos los niveles instituciones eficaces e inclusivas que rindan cuentas. Observaciones generales del Examen Periódico Universal: N.º 16: Derecho a la intimidad (artículo 17) y Observación General N.º 35: Libertad y seguridad personales. Ministerio de Relaciones Exteriores de Paraguay - Sistema SIMORE, etiqueta "Vigilancia", "Examen Periódico Universal", acceso el 5 de octubre de 2020, https://www.mre.gov.py/simoreplus/ (etiqueta vigilancia).

16 "Solicitud #33586". Informe sobre Examen Periódico Universal de Naciones Unidas (EPU)", Portal Unificado de Información Pública, acceso el 8 de octubre de 2020, https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/33586.

17 "Solicitud #34610. Examen Periódico Universal de las Naciones Unidas (EPU), Ministerio del Interior", Portal Unificado de Información Pública, acceso el 17 de septiembre de 2020, https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/34610.

18 "Solicitud #34609. Examen Periódico Universal de las Naciones Unidas (EPU), Senad", Portal Unificado de Información Pública, acceso el 17 de septiembre de 2020, https://informacionpublica.paraguay.gov.py/portal/#!/ciudadano/solicitud/34609.

19 Principales elementos de la consulta de Tedic al Ministerio del Interior y Senad:
1. Detallar las medidas y protocolos necesarios que se están llevando a cabo sobre el funcionamiento de las agencias de inteligencia: Sistema Nacional de Inteligencia (Sinai), Ministerio del Interior y Secretaría Nacional Antidrogas (Senad). Adjuntar copia de las resoluciones que detallen el tipo de tecnología que se utiliza y cómo se utilizan u otro funcionario que describa la tecnología y su funcionamiento.
2. Informar los detalles de implementación, protocolos y cualquier tipo de tratamiento de datos personales de las personas que se utilizan en el sistema de vigilancia de las agencias de inteligencia.
3. Detallar las medidas y protocolos necesarios para garantizar la transparencia y rendición de cuentas para que sean supervisados por mecanismos de seguimiento independientes. Adjuntar copia de las resoluciones que detallan estos protocolos para garantizar transparencia y rendición de cuentas.

tecnologías. La Asociación Tedic ha interpuesto una acción de inconstitucionalidad contra la respuesta a la solicitud pública Resolución N.º 238 del Ministerio del Interior y las consecuentes resoluciones judiciales que validaron dicha decisión. El Poder Judicial ha rechazado en las dos primeras instancias el acceso a la información pública, argumentando que entra en el ámbito de seguridad nacional, a pesar de que la ley establece claramente que el carácter de reservado debe estar expresamente establecido en la ley (art. 22 de la Ley N.º 5282/2015). Este no es el caso, pues no existe normativa legal alguna que reserve el tipo de información requerida. Hasta la fecha, no se ha resuelto la acción y el caso se encuentra hace más de un año en la Corte Suprema de Justicia (CSJ)[20].

Hasta el presente, el Paraguay no cuenta con un marco legal de protección integral de datos personales. Ello implica una falta de garantías de protección ante posibles abusos en el tratamiento de datos personales tanto en instituciones del sector público como privado. Esto ha provocado el almacenamiento, registro y utilización de datos personales y sensibles de forma indiscriminada. Esta preocupación se viene exponiendo en todos los informes anuales y recién este año 2020 aparece una tímida apertura para su discusión en el Congreso Nacional[21].

VIOLENCIA DE GÉNERO EN LÍNEA

La ONG Luchadoras de México define a la violencia en línea como "actos de violencia de género cometidos instigados o agravados, en parte o totalmente, por el uso de las Tecnologías de la Información y la Comunicación (TIC), plataformas de redes sociales y correo electrónico. Estas violencias causan daño psicológico y emocional, refuerzan los prejuicios, dañan la reputación, causan pérdidas económicas y plantean barreras a la participación en la vida pública y pueden conducir a formas de violencia sexual y otras formas de violencia física"[22]. En ese sentido, cabe mencionar en primer lugar que falta mucho camino por recorrer, pues no se considera que las TIC incidan en la desigualdad de género ni que reproduzcan y/o refuercen la violencia. Ejemplo de ello es la definición incompleta de esta violencia que se encuentra en la mencionada Ley N.º 5777/2016[23]. Si bien acogemos con agrado el hecho de

20 "¿Quién vigila al vigilante? Reconocimiento facial en Asunción - Paraguay", *Blog de Tedic*,16 de septiembre de 2019, https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion.

21 "Inició el ciclo de charlas de la Coalición de Datos Personales", 10 de junio de 2020, *Blog de Tedic*, https://www.tedic.org/inicio-el-ciclo-de-charlas-de-la-coalicion-de-datos-personales/.

22 Luchadoras de México, *La violencia en línea contra las mujeres en México* (México: Luchadoras de MX, 2017), https://luchadoras.mx/wp-content/uploads/2017/12/Informe_ViolenciaEnLineaMexico_InternetEsNuestra.pdf.

23 Artículo 6, inciso I: **Violencia telemática.** Es la acción por medio de la cual se difunden o publican mensajes, fotografías, audios, videos u otros que afecten la dignidad o intimidad de las mujeres a través de las actuales tecnologías de información y comunicación, incluido el uso de estos medios para promover la cosificación, sumisión o explotación de la mujer. Se entenderá por "cosificación" a la acción de reducir a la mujer a la condición de cosa.

que este tipo de violencia haya sido incluido en la ley, su definición es incompleta, ya que se enfoca únicamente en la difusión de imágenes no consensuadas y la exposición por los medios de comunicación; dejando de lado el acoso en línea, las amenazas, el seguimiento y el acecho, las expresiones discriminatorias, el descrédito, el acceso no autorizado, la suplantación / robo de identidad, el abuso y la explotación sexual relacionados con las tecnologías, afectando los canales de expresión y omisiones de los actores con poder regulatorio. Ello, de acuerdo con lo identificado como tipos de violencia en línea en informes realizados por la sociedad civil, como ser el de la Asociación para el Progreso de las Comunicaciones (APC) y Luchadoras de México[24], que identifica 13 tipos de violencia en línea. Esta falta de consideración da como resultado que ciertas formas de violencia que forman parte de la violencia en línea se vuelvan invisibles y, por tanto, desprotegidas. Como resultado, actualmente no existen estudios ni puntos de referencia epistémicos que den cuenta del problema en sí en Paraguay; tampoco existe producción de datos representativos en el observatorio de género[25] (perteneciente al Ministerio de la Mujer) referente a este tipo de violencias, por lo que no se generan capacidades institucionales que habiliten políticas públicas para salvaguardar, proteger y reparar a las personas víctimas de esta violencia.

A su vez, preocupa que las violaciones a derechos de las mujeres ocurridas en espacios digitales, además de no ser reconocidas en su totalidad, resultan en una negativa sistemática de justicia en el Poder Judicial. La legislación preexistente a la Ley N.º 5777/2016, así como la legislación penal y los tratados internacionales de derechos humanos no son aplicados de igual forma a las violencias ocurridas en los espacios digitales, a pesar de que las acciones se subsuman en los tipos legales ya existentes, como es el caso del "acoso sexual", reconocido en el artículo 133 del Código Penal Paraguayo[26].

CASO BELÉN WHITTINGSLOW. Este caso configura violencia de género en línea e ilustra la falta de independencia judicial y acceso a la justicia en Paraguay. Belén Whittingslow denunció a Cristian Kriskovich, profesor de la Universidad Católica de Asunción y representante de la misma ante el Consejo de la Magistratura, órgano central en el proceso de designación y nombramiento de jueces y agentes fiscales[27], y el Jurado de Enjuiciamiento de Magistrados, órgano con facultades para sancionar a magistrados y agentes fiscales[28] por

24 "13 formas de agresión relacionada con las tecnologías contra las mujeres", *Luchadoras de México*, acceso el 1 de octubre de 2020, https://luchadoras.mx/13-formas-violencia-linea-las-mujeres/.

25 El Observatorio para las Mujeres es un espacio de la Secretaría Nacional de Tecnologías de la Información y Comunicación (actualmente Ministerio de las Tecnologías de la Información y Comunicación), para el seguimiento de casos de violencia hacia las mujeres, al que puede accederse desde su sitio web: http://observatorio.mujer.gov.py/.

26 **"Artículo 133. Acoso sexual 1.º:** El que con fines sexuales hostigara a otra persona, abusando de la autoridad o influencia que le confieren sus funciones, será castigado con pena privativa de libertad de hasta dos años. **2.º:** En estos casos se aplicará lo dispuesto en el artículo 59. **3.º:** La persecución penal dependerá de la instancia de la víctima".

27 Artículo 264 de la Constitución Nacional del Paraguay.

28 Artículo 11 de la Ley N.º 3759/2009.

acoso sexual (llevado a cabo a través de medios digitales). Ella terminó siendo solicitante de refugio en Uruguay tras haber sido perseguida judicialmente.

Los hechos denunciados por Belén se remontan al año 2013, cuando alegó que, siendo alumna del Sr. Kriskovich, este la acosó sexualmente por medios digitales, a través de mensajes e imágenes enviados por la aplicación de mensajería instantánea WhatsApp[29]. A pesar de haberse ordenado la realización de la pericia de los celulares –principal prueba del acoso denunciado–, tras un escrito presentado por la defensa del Sr. Kriskovich, el fiscal del caso decidió desconvocar las diligencias de la pericia y desestimar la causa[30]. Tal decisión fue ratificada por el fiscal adjunto, quien consideró que el hecho denunciado no configuraba acoso sexual, calificándolo como "galanteo o cortejo"[31] en una resolución *contra legem*. Es así como, en este proceso, el Ministerio Público desestimó por completo la oposición de Belén a los mensajes recibidos (plasmada en los mensajes ofrecidos como prueba en el expediente) en base a argumentos sustentados en prejuicios de género y evitando analizar la posición de poder ostentada por el Sr. Kriskovich[32].

Luego de la desestimación, Belén fue involucrada en dos procesos judiciales en su contra, que continúan aún hoy, 6 años después. Estos procesos han estado plagados de irregularidades y violaciones al debido proceso, tales como la cancelación de la defensa y la solicitud de orden de captura contra la víctima tras una declaración de rebeldía, que carece de fundamentos legales[33]. Este caso pone de relieve dos temas fundamentales en Paraguay: por un lado, la marcada discriminación, estigmatización y denegatoria de justicia, que afecta a las mujeres que denuncian el acoso sexual y la violencia de género. Por otro, los obstáculos judiciales que aparecen a la hora de buscar justicia y reparación en casos que la violencia de género se da a través de medios digitales.

SITUACIÓN DEL DERECHO EN 2020

DRONES EN TIEMPOS DE EMERGENCIA SANITARIA

El Ministerio del Interior adquirió drones para la vigilancia de espacios públicos para fiscalizar el cumplimiento del confinamiento obligatorio en tiempos de pandemia. No es la primera vez que esta institución obtiene tecnología para la vigilancia no tripulada: en 2019 ya había adquirido un ve-

29 Causa N.º 8830/2014, caratulada "Cristian Kriskovich S/ Acoso Sexual".

30 Resolución N.º 9 del 23 de abril de 2015, proferida por el fiscal Centurión, Causa N.º 8830/2014.

31 Dictamen N.º 735, proferido por el fiscal adjunto Jorge Sosa, folios 4 y 5, Causa N.º 8830/2014.

32 Dictamen N.º 735 del 1 de junio del 2015, proferido por el fiscal adjunto Jorge Sosa, Causa N.º 8830/2014.

33 Causa N.º 2882/2014, caratulada "Víctor David Arce Y Otros S/ Producción De Documentos No Auténticos".

hículo no tripulado[34]. El entonces ministro, Juan Ernesto Villamayor, había señalado que el objetivo de dicha licitación era utilizar el dron en manifestaciones, desalojos de inmuebles, allanamientos y eventos deportivos[35].

El uso de tecnologías digitales para combatir la pandemia no puede quedar excluido de un examen de necesidad y proporcionalidad ante eventuales afectaciones a los derechos fundamentales. En esta línea, toda tecnología utilizada en el contexto de pandemia, como el uso de un dron, debe priorizar la protección de los datos personales y sensibles, así como garantizar un uso acotado –a la emergencia sanitaria actual– y habilitar procedimientos de rendición de cuentas. Todas estas medidas son claves para evitar impactos desproporcionados en la discriminación de los grupos en situación de mayor vulnerabilidad, así como posibles impactos en la salud mental y en la estigmatización de las personas afectadas por la covid-19. Esto se remarca en las recomendaciones sostenidas por la Resolución N.º 1/2020 de la Comisión Interamericana de Derechos Humanos (CIDH) sobre "Pandemia y Derechos Humanos en América"[36].

DISPOSITIVOS ELECTRÓNICOS DE CONTROL: PARCHES LEGALES

El Poder Legislativo sancionó la Ley N.º 6558/2020 que modifica la "Ley contra la Violencia Doméstica"[37]. La misma ley habilita al juez a imponer medidas de vigilancia, como el sistema de monitoreo por dispositivos electrónicos de control, que permitan el reconocimiento de ubicación del agresor, de modo a realizar un seguimiento y control.

La propuesta legal es legítima. Sin embargo, pone en riesgo a la víctima, ya que, para identificar la proximidad del agresor, esta persona también debería facilitar su localización a la Policía Nacional[38].

34 "Adjudicación de la Licitación 368495 - Adquisición de vehículo aéreo no tripulado (UAV / DRON) y lanzador semiautomático de proyectiles no letales (balines de goma)", *Dirección Nacional de Contrataciones Públicas*, 4 de octubre de 2019, acceso el 30 de septiembre de 2020, https://www.contrataciones.gov.py/licitaciones/adjudicacion/368495-adquisicion-vehiculo-aereo-no-tripulado-uav-dron-lanzador-semiautomatico-proyectiles-1/resumen-adjudicacion.html.

35 "Drone Use: Does It Combat the Pandemic or Strengthen Surveillance?", *Blog de Tedic*, 9 de julio de 2020, https://www.tedic.org/en/drone-use-does-it-combat-the-pandemic-or-strengthen-surveillance/.

36 Adoptada por la CIDH el 10 de abril de 2020, http://oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf.

37 Ley N.º 6568, del 26 de junio de 2020, que modifica el artículo 2.º de la Ley N.º 1600/2000 "Contra la violencia doméstica", *Biblioteca y Archivo Central del Congreso de la Nación*, https://www.bacn.gov.py/leyes-paraguayas/9284/ley-n-6568-modifica-el-articulo-2-de-la-ley-n-16002000-contra-la-violencia-domestica.

38 "Sancionan uso de tobilleras electrónicas para casos de violencia doméstica", *Última Hora*, 16 de junio de 2019, acceso el 26 de septiembre de 2020, https://www.ultimahora.com/sancionan-uso-tobilleras-electronicas-casos-violencia-domestica-n2890499.html.

SUPERPODERES PARA LA POLICÍA NACIONAL

Por otro lado, la Comisión Nacional de Telecomunicaciones (Conatel) dictó la Resolución N.º 583/2020, por la cual "se modifica el reglamento de protección al usuario de telecomunicaciones"[39], con el fin de prevenir el fraude y la extorsión. Con esta norma se faculta al Ministerio del Interior a solicitar el bloqueo de líneas telefónicas sin autorización judicial, ni cumplimiento del debido proceso.

Por su parte, las operadoras de servicios de telefonía de Paraguay se mostraron preocupadas por la normativa y solicitaron una revisión del marco legal.

Hasta la fecha no hay respuesta por parte de las autoridades de Conatel.

CIBERPATRULLAJE EN TIEMPOS DE PANDEMIA Y VIGILANCIA EN PROTESTAS PACÍFICAS

La Fiscalía de Delitos Informáticos imputó a una persona por la supuesta amenaza de contagiar covid-19. El hecho ocurrió en la red social Twitter cuando la persona publicó la siguiente frase: "Te vamos a entregar el virus en *delivery*"[40].

La Fiscalía también realizó audiencias indagatorias e imputó a manifestantes que protestaban pacíficamente por el asesinato de dos niñas a manos de la Fuerza de Tarea Conjunta (FTC)[41]. La causa de la imputación tiene que ver con la violación de vedas y cuarentenas sanitarias, prevista en el artículo 10 inciso b de la Ley N.º 716/1996 "Que sanciona delitos contra el medio ambiente"[42]. También utilizó imágenes publicadas en redes sociales para identificar a las personas que estuvieron en una manifestación pública contra el Estado, que tuvo como desencadenamiento el daño con pintura a un monumento

39 "Resolución de directorio N.º 584/2020", *Blog de Conatel*, febrero de 2020, https://www.conatel.gov.py/conatel/resolucion-directorio-n-24-2020-2/.

40 "Imputan a mujer que habló de 'entregar el virus en delivery' en Twitter", *ABC Color*, 31 de marzo de 2020, acceso el 20 de septiembre de 2020, https://www.abc.com.py/nacionales/2020/03/31/mujer-que-amenazo-con-contagiar-covid-19-se-expone-a-pena-de-tres-anos/.

41 Claudia Korol, "¡Eran niñas!: el doble infanticidio en Paraguay | Sobre los crímenes de María del Carmen Villalba y Lilian Villalba en Paraguay", *Página 12*, 11 de septiembre de 2020, acceso el 13 de septiembre de 2020, https://www.pagina12.com.ar/291213-eran-ninas-el-doble-infanticidio-en-paraguay.

42 Causa N.º 5616/2020 "Paloma Chaparro y otras s/ S. H. P. Daños a cosas de interés común y otros, transgresión de la Ley N.º 716/1996 Delitos contra el medio ambiente en vedas y cuarentenas", ante la Unidad Penal N.º 1 Especializada en Seguridad y Convivencia entre las Personas y la Unidad Penal Ordinaria N.º 2 de la Sede N.º 1 Capital.

nacional[43] [44] [45]. Entre otras observaciones preocupantes, está el hecho de que en la carpeta fiscal no se percibe ningún proceso legal de obtención de estos metadatos vía autorización judicial. Cabe resaltar que, según la Constitución Nacional en su artículo 36, la interceptación de las comunicaciones (en esto se incluyen los metadatos de una comunicación) solo se realiza vía solicitud judicial.

Las actividades de recolección de información a granel, de manera previa y sin una investigación asociada a un hecho punible, son problemáticas. Existe una fina línea que divide lo que es una actividad de vigilancia generalizada, de una actividad de inteligencia para la prevención específica de delitos.

El ciberpatrullaje no se puede homologar al patrullaje físico, porque los efectos de prevención y disuasión de este se relacionan más con la presencia visual de la autoridad. En el ámbito digital únicamente puede ser vigilancia, pues no tiene sentido hacerla azarosamente, sino de forma direccionada. ¿Con qué criterios se observan los perfiles, identidades o *hashtags*? Por tanto, estas técnicas no pueden ser consideradas patrullaje, sino que conforman mecanismos de vigilancia desproporcionada e innecesaria.

DATOS PERSONALES SENSIBLES Y SALUD

El Ministerio de Salud, en su Resolución S. G. N.º 146/2012 (artículos 4 y 6) afirma que existe la obligación de respetar y proteger el derecho a la intimidad, así como la obligación de todo personal de salud a respetar el carácter confidencial de la información y datos de todas las personas que reciben atención en salud o acuden para recibir información y orientación en un servicio de salud[46]. Por lo tanto, no debe utilizarse como justificación la salud para socavar y restringir desproporcionadamente los derechos y las libertades fundamentales.

En el contexto de la pandemia de covid-19, iniciada en marzo de 2020, se desató un miedo generalizado en la población y las respuestas a menudo fueron reacciones violentas y discriminación. La información de carácter

43 Causa N.º 5616/2020 "Paloma Chaparro y otras s/ S. H. P. Daños a cosas de interés común y otros, transgresión de la Ley N.º 716/1996 Delitos contra el medio ambiente en vedas y cuarentenas", ante la Unidad Penal N.º 1 Especializada en Seguridad y Convivencia entre las Personas y la Unidad Penal Ordinaria N.º 2 de la Sede N.º 1 Capital.

44 "Más imputados por actos frente al Panteón y piden tener más fiscales", *Última Hora*, 16 de septiembre de 2020, acceso el 18 de septiembre de 2020, https://www.ultimahora.com/mas-imputados-actos-frente-al-panteon-y-piden-tener-mas-fiscales-n2905031.html.

45 "La parcialidad de la Fiscalía lleva a peligrosas prácticas stronistas", *Última Hora*, 17 de septiembre de 2020, acceso el 18 de septiembre de 2020, https://www.ultimahora.com/la-parcialidad-la-fiscalia-lleva-peligrosas-practicas-stronistas-n2905243.html.

46 "La privacidad e intimidad de pacientes es un derecho que se protege desde el MSP", *Ministerio de Salud Pública y Bienestar Social*, 24 de junio de 2015, acceso el 25 de septiembre de 2020, https://www.mspbs.gov.py/portal/5514/la-privacidad-e-intimidad-de-pacientes-es-un-derecho-que-se-protege-desde-el-msp.html.

sensible sobre personas que tuvieron la enfermedad fue filtrada –tanto en el sistema de salud público como privado–, lo que provocó casos de persecuciones públicas[47].

El Mitic desarrolló una aplicación móvil para registro y seguimiento de síntomas de personas con covid-19. Según el Ministerio de Salud, 5.473 personas la descargaron[48], aunque solo se les dé el alta en el sistema a personas que dan positivo. Hasta la fecha no se pudo acceder a las políticas de privacidad y tratamiento de datos, así como la posibilidad de aplicar los derechos ARCO[49] para eliminar su perfil, una vez finalizada la etapa crítica de la pandemia.

Por otro lado, se busca crear la historia clínica electrónica en Paraguay a través de una propuesta legislativa que se encuentra en análisis en el Congreso y pretende que el registro de documentos sea obligatorio, cronológico, individualizado y completo en soporte digital y propiedad del paciente. A su vez, se prevé que cada actuación médica conste en forma de escritos, gráficos e imagenológicos o de cualquier otra índole realizada a una persona, desde el nacimiento hasta el fallecimiento[50]. Al cierre de este informe, no existe un análisis previo del posible impacto en los derechos humanos. En vista de que no existe una la ley que resguarde los datos personales, no parece haber garantías de protección ante posibles abusos de esta información sensible.

SISTEMAS DE AYUDA ÑANGAREKO Y PYTYVÕ

Los sistemas de ayuda económica y kits de alimentos del Estado para grupos en situación de vulnerabilidad en tiempos de pandemia, denominados Ñangareko y Pytyvõ, tuvieron varias debilidades en su implementación, provocando la vulneración de información sensible de las personas beneficiarias. Se filtraron bases con datos personales, así como la información sobre el cobro de recursos económicos por terceras personas que se hacían pasar por beneficiarias[51]. Estas bases se encuentran alojadas en servidores de empresas privadas y sus páginas web no cuentan con criterios mínimos de seguridad, como el protocolo seguro de transferencia (HTTPS). El riesgo es

47 "Familia de paciente con Covid-19 recibe amenazas", *Última Hora*, 16 de marzo de 2020, acceso el 20 de marzo de 2020, https://www.ultimahora.com/familia-paciente-covid-19-recibe-amenazas-n2875197.html.

48 Según datos obtenidos por Tedic en consulta al MSPyBS, de este total, 2.484 son mujeres y 2.989 son varones.

49 Los derechos ARCO son el conjunto de acciones por las cuales una persona física puede ejercer el control sobre sus datos personales. Son seis: Acceso, Rectificación, Cancelación, Oposición, Limitación y Portabilidad.

50 Lic. Nilza Florentín, "Legisladores proponen crear registro de historias clínicas electrónicas", *Cámara de Senadores*, 16 de junio de 2020, acceso el 29 de septiembre de 2020, http://www.senado.gov.py/index.php/noticias/noticias-generales/5900-legisladores-proponen-crear-registro-de-historias-clinicas-electronicas-2020-06-16-22-55-57.

51 "Pytyvõ: Policía descarta hackeo e investiga quiénes filtraron datos de beneficiarios", *Última Hora*, 2 de junio de 2020, acceso el 5 de junio de 2020, https://www.ultimahora.com/pytyvo-policia-descarta-hackeo-e-investiga-quienes-filtraron-datos-beneficiarios-n2888246.html.

que estas bases de datos puedan ser utilizadas con fines políticos, ya que no existen control ni transparencia en la recolección de la información.

La digitalización de los servicios públicos puede afectar negativamente a las personas y comunidades que ya están en situación de desventaja (incluidas quienes se encuentran en situación de desventaja debido a su condición económica, social, de clase o jurídica, entre otros factores), a quienes dependen del Estado para su sustento y el de sus familias y dependientes, así como a las comunidades y personas que ya estaban marginadas y han sido las más duramente golpeadas por las medidas de digitalización de los servicios, en el marco de la emergencia sanitaria.

PROTECCIÓN DE DATOS PERSONALES

Actualmente, hay actores políticos interesados que han comenzado, junto con la Coalición de Datos Personales[52], la elaboración de un borrador de ley integral de datos personales en Paraguay.

Esto no solamente ofrecerá protección de los derechos humanos, sino también seguridad legal para empresas locales, así como para que empresas globales de tecnología puedan instalarse y realizar tratamiento de datos transfronterizos con reglas acordes a los estándares internacionales.

CONCLUSIONES

Como se viene insistiendo desde hace 5 años en cada informe anual, se evidencia la incapacidad del Estado paraguayo de garantizar y proteger la vida privada de las personas en el entorno en línea.

Se observa una tendencia con enfoque de políticas públicas tecnosolusionistas, donde no aparecen los análisis de impacto en general y en particular sobre posibles afectaciones a los derechos humanos. Las instituciones del Estado no han logrado incluir en sus marcos normativos enfoques centrados en la persona, para elevar la calidad de vida en general y ejercer plenamente los derechos de las personas en el entorno en línea. Esto se manifiesta en el aumento de capacidades de las instituciones del Estado para perseguir delitos y crímenes, pero sin un marco legal basado en el derecho internacional de los derechos humanos, ni en las recomendaciones de organismos internacionales que se encargan de temas como libertad de expresión y privacidad en Internet.

52 Conformada por Tedic, Asociación Paraguaya de Derecho Informático y Tecnógico (Apadit), Fundación Paraguay Ciberseguro, Internet Society - Paraguay Chapter y Abente Stewart Abogados. Más datos en https://www.datospersonales.org.py.

Entre algunos de los obstáculos que se pueden visualizar como estancamiento, es posible mencionar, por un lado, la existencia de un concepto erróneo sobre el uso y las consecuencias de la tecnología por parte de la ciudadanía y de los políticos que ocupan cargos en el poder como legisladores y jueces. Esto, por lo general, tiene consecuencias negativas en la generación de normativas y prácticas legales contrarias a los derechos humanos.

Por otro lado, se encuentran la precaria infraestructura de Internet y los altos costos para acceder a esta tecnología, generando brechas digitales y de género a través de políticas públicas "parches" para la inclusión digital de mujeres y comunidades vulnerables. Usar productos tecnológicos no solamente representa ganancias para las industrias tecnológicas en este rubro, sino que se pierde el norte de una verdadera política pública basada en contextos locales y generando daños colaterales como la brecha digital.

Además, existe una gran opacidad por parte de las instituciones de vigilancia del Estado en cuanto a la transparencia y rendición de cuentas de sus adquisiciones y procesos de vigilancia de las comunicaciones. Año tras año se observa cómo se amplían las capacidades del Estado en materia de vigilancia de las comunicaciones a través de nuevas normativas y adquisiciones de *software* y *hardware* de vigilancia. Esto tiene como consecuencia una intromisión en la vida de las personas, que no se adecua a las pautas sugeridas por los estándares internacionales de derechos humanos y las relatorías especiales de los organismos internacionales como la ONU y la OEA (Organización de Estados Americanos).

Finalmente, en cuanto a las acciones en tiempos de emergencia sanitaria, es indiscutible que la tecnología puede ayudar a que el Gobierno sea capaz de dar respuestas y resolver algunos de los desafíos fundamentales que enfrentan al hacerlo, con el fin de garantizar que las personas y las comunidades vivan con dignidad, a partir de algunas políticas como los programas de ayuda. Sin embargo, el Estado debe tener en cuenta, desde el inicio de estas soluciones tecnológicas, las salvaguardas y las garantías para ofrecer servicios digitales a una población desconectada. Asimismo, es indispensable insertar en sus políticas de inclusión digital y el desarrollo de tecnología para mitigar la covid-19, una evaluación previa de los principios de proporcionalidad y necesidad. En la experiencia expuesta en este artículo no quedan claros muchos criterios, entre ellos la duración del tratamiento de datos personales sensibles luego de que termine la emergencia.

RECOMENDACIONES

El Estado paraguayo debe:

a. En referencia a la vigilancia:

→ adoptar una normativa específica sobre el uso de herramientas de vigilancia como piratería, *malware*, drones o tecnologías biométricas, teniendo en cuenta los principios de necesidad y proporcionalidad.

→ elaborar mecanismos de control y autorización judicial independientes.

→ establecer regulaciones que aseguren que el uso de tecnología de vigilancia privada sea auditable por órganos de supervisión.

→ brindar transparencia acerca de las capacidades generales de vigilancia del Estado e información significativa sobre el alcance en el uso de tecnología de vigilancia privada.

→ asegurar que las personas que son objetivo de las tecnologías de vigilancia sean notificadas y tengan acceso a garantías de protección.

→ garantizar la existencia de órganos de control independientes e imparciales, dotados de las facultades necesarias para auditar, investigar y perseguir eficazmente cualquier abuso en el uso de tecnologías de vigilancia por parte de actores estatales. Esto incluye tener acceso absoluto a cualquier información, instalaciones o equipos necesarios para el desempeño de sus funciones.

→ adoptar medidas de debida diligencia en materia de derechos humanos en la adquisición de tecnologías de vigilancia, con el fin de evaluar y monitorear posibles abusos o violaciones a los derechos humanos en el despliegue de dichas tecnologías.

→ fiscalizar a las empresas que despliegan tecnologías de vigilancia privada en su propio beneficio con el propósito de vulnerar derechos humanos o socioambientales e imponer las sanciones oportunas.

b. En cuanto a la violencia de género en línea:

→ generar políticas públicas para sensibilizar sobre la violencia de género en línea.

→ promover la modificación de la Ley N.º 5777/16, artículo 6 inc. l para incluir las diversas violencias contra las mujeres que constituyen violencia telemática.

→ adoptar medidas inmediatas y eficaces para prevenir y dar respuesta a todas las formas de violencia contra las mujeres en contextos digitales, eliminando el machismo de la administración de justicia y garantizando que todas las personas involucradas en actos de violencia contra las mujeres y niñas rindan cuentas de sus actos y sean llevadas ante la Justicia.

→ garantizar una investigación efectiva, independiente e imparcial de las denuncias de violaciones de derechos humanos de las mujeres en línea.

→ adoptar las medidas necesarias para asegurar el acceso a un recurso efectivo en casos de violencia de género en línea, respetando sus compromisos en materia de derechos humanos.

→ impulsar las medidas necesarias para la resolución de la acción de inconstitucionalidad presentada e investigar a jueces y fiscales que han sido denunciados por mal desempeño de sus funciones en el caso de Belén Whittingslow.

c. Sobre la protección de datos personales en línea:

→ promulgar una ley integral de datos personales en Paraguay para garantizar y resguardar la vida privada de las personas en el entorno en línea, de acuerdo con los más altos estándares de derechos humanos y protección de datos, así como crear una autoridad independiente para la supervisión, el control y la rendición de cuentas.

d. En relación con las aplicaciones creadas para enfrentar la pandemia:

→ asegurar que las aplicaciones que aborden situaciones de emergencia sanitaria puedan surgir de su uso y su impacto potencial en el ejercicio de cualquier medida extraordinaria adoptada para responder y abordar la pandemia por covid-19, y estén en línea con las leyes y los estándares de derechos humanos, además de ser temporales y limitadas en el tiempo de la duración de esta.