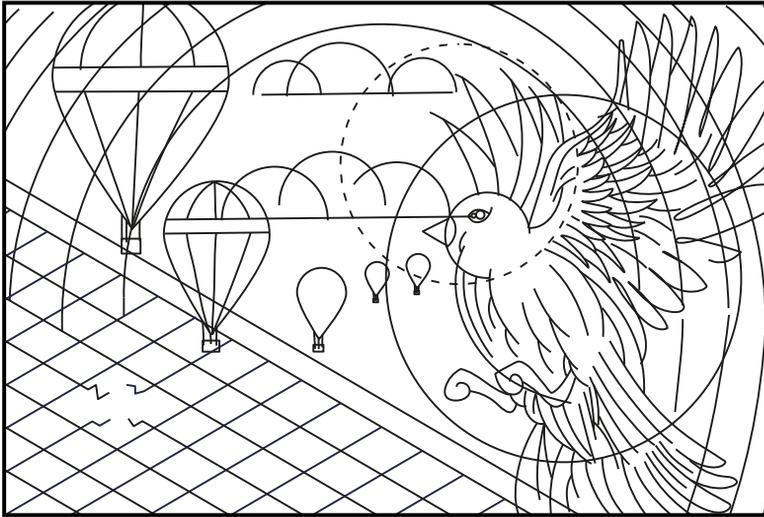


DERECHOS DIGITALES

LA HEREJÍA TECNO-OPTIMISTA FLORECE DURANTE LA PANDEMIA



El Estado paraguayo sigue adoptando tecnologías para implementar políticas públicas sin un enfoque de derechos humanos. Así, se abre la posibilidad de abusos contra la población, en especial, sectores vulnerables. Se amplían la brecha digital, las desigualdades, la discriminación y la violación de derechos esenciales. El Gobierno debe enfrentar el reto de garantizar la protección y la seguridad en el entorno digital. Y esto incluye atender la desprotección de las mujeres en un marco de creciente violencia digital de género.

Palabras claves: *privacidad, datos personales, libertad de expresión, neutralidad en la red, género e Internet.*

Maricarmen Sequera y Eduardo Carrillo

TEDIC

El presente artículo ofrece un recuento de iniciativas tecnológicas del Estado paraguayo y su impacto en el disfrute de los derechos humanos. Concretamente, resalta los peligros de adoptar tecnologías con fines de vigilancia y recolección masiva de datos sensibles. Destaca también los riesgos y oportunidades de la ley del teletrabajo y denuncia censura en línea en la zona norte del país. También se resalta la importancia de la protección de los datos personales y documenta el actual estado en materia de violencia de género en línea. Ofrece, por último, una serie de recomendaciones para mitigar situaciones de abuso y discriminación.

SITUACIÓN DEL DERECHO

BRECHA EN AUMENTO, A PESAR DE LOS AVANCES TECNOLÓGICOS

Los principales debates globales sobre los derechos humanos en Internet están centrados en las tensiones y los conflictos que se generan en los entornos digitales. Habitualmente, la tecnología es presentada como la solución eficiente a problemas sociales en donde la desigualdad es moneda corriente. Aquellos que promueven este tipo de discursos fomentan lo que se conoce como solucionismo tecnológico o tecno-optimismo¹. Es decir, se piensa a la tecnología como un igualador de oportunidades, sin detenerse en los contextos culturales, sociales y económicos que atraviesan a cada sociedad. La brecha entre ricos y pobres va en aumento², a pesar de las constantes innovaciones tecnológicas, una situación que se agravó con la pandemia derivada del COVID-19. Por tanto, todas las políticas públicas y legislaciones nacionales que buscan innovar, adquirir, implementar y vender soluciones tecnológicas deben incluir evaluaciones de impacto de derechos humanos.

En los últimos años, el Estado paraguayo ha implementado con mucha carencia y desconocimiento las políticas con enfoque de derechos en la tecnología: generando más brecha digital, desigualdades, discriminación y violaciones de derechos fundamentales. Ejemplo de ellos son los bloqueos de acceso a Internet de comunidades vulnerables, la vigilancia y el control biométrico sin rendición de cuentas, y la vigilancia a connacionales y migrantes en zonas de fronteras. A su vez, existen leves parpadeos hacia una regulación que proteja a toda la población: campañas contra la violencia digital, leyes laborales que incluyen el derecho a la desconexión, proyectos de ley de protección de datos personales, entre otros.

1 Evgeny Morozov, *La locura del solucionismo tecnológico* (Buenos Aires: Katz Editores y Capital Intelectual, 2015).

2 Maricarmen Sequera, «Educación virtual y la infraestructura de Internet en Paraguay», TEDIC, 27 de abril de 2020, <https://www.tedic.org/la-educacion-virtual-y-la-infraestructura-de-internet-en-paraguay/>

MÁS SUPERPODERES A LA POLICÍA NACIONAL

Desde hace varios años, TEDIC³ reporta las nuevas adquisiciones de tecnología de vigilancia y nuevas atribuciones de control de la Policía Nacional. Entre algunas de ellas se encuentran los *malware* de vigilancia remota, drones de vigilancia en espacios públicos, reconocimiento facial en las calles y ciberpatrullajes en redes sociales⁴. Se amplían las atribuciones de la Policía Nacional con serios problemas de cumplimiento del debido proceso, tales como los bloqueos al acceso a telefonía móvil sin orden judicial, vigilancia de las comunicaciones sin protocolos de transparencia y rendición de cuenta, entre otros⁵. Estas mismas preocupaciones fueron observadas por los países que analizaron el Examen Periódico Universal (EPU) de Paraguay en el ciclo anterior al de este año, en donde recomendaron una evaluación de impacto de derechos humanos⁶ con los estándares de proporcionalidad y necesidad⁷.

Sin embargo, la implementación de tecnología en los sistemas de control del Estado sigue haciendo oídos sordos a las recomendaciones del EPU e inquietudes de la sociedad civil sobre los estándares de derechos humanos. Este año, la Comandancia de la Policía Nacional anunció la utilización del sistema biométrico AFIS (identificación automática por huellas dactilares) para realizar un control aleatorio de personas que emplean los medios de transporte público en Asunción⁸. Según la Policía Nacional, este procedimiento de control aleatorio ha colaborado en la identificación de personas con orden de captura⁹. Por otra parte, se revela una tendencia a la adquisición de cámaras corporales¹⁰ a ser utilizadas por agentes policiales e invocando argumentos de control y cumplimiento del protocolo sanitario

3 <https://www.tedic.org/>

4 Maricarmen Sequera y Paloma Lara Castro Escobar, «Derechos Digitales en modo Covid-19», en *Derechos Humanos en Paraguay 2020* (Asunción: Codehupy, 2020), 373-389.

5 *Ibidem*.

6 «102.62: Velar por que todas las actividades de vigilancia del Estado estén en consonancia con el derecho internacional de los derechos humanos y no infrinjan los derechos y libertades fundamentales del ciudadano» (recomendación de Liechtenstein, EPU, 2016), *Simore Plus*, <https://www.mre.gov.py/SimorePlus/Home/resultado>

7 «Necesarios&Proporcionados. Sobre aplicación de los derechos humanos a la vigilancia de las comunicaciones», *Electronic Frontier Foundation*, <https://necessaryandproportionate.org/es/13-principles/>

8 «Controles en colectivos serán a través de sistema de huellas AFIS», *ABC Color*, 9 de septiembre de 2021, acceso el 15 de octubre de 2021, <https://www.abc.com.py/nacionales/2021/09/09/controles-en-colectivos-seran-a-traves-de-sistema-de-huellas-afis/>

9 «Detienen a un hombre que contaba con cuatro órdenes de captura en su contra», *Última Hora*, 15 de septiembre de 2021, acceso el 15 de octubre de 2021, <https://www.ultimahora.com/detienen-un-hombre-que-contaba-cuatro-ordenes-captura-su-contra-n2961542.html>

10 «Llamado a Contratación», *Contrataciones Públicas*, 11 de agosto de 2021, acceso el 15 de octubre de 2021, https://www.contrataciones.gov.py/sicp/llamado/llamadoPublico.seam;jsessionid=5CoB1tEC1A1038CE126533425A7BAA5A.jbos15?_llamadold=IaoDGBIPlzA%3D&conversationPropagation=end&actionMethod=llamado%2FllamadosPublicados.xhtml%3AllamadoPublicoAction.initFromGridPublico&cid=111742

vigente¹¹ y para evitar situaciones posibles de coima o abuso policial en intervenciones¹².

Lo anterior se conecta con una visión y un modelo de seguridad planteado por el actual ministro del Interior, quien ha expresado a inicios de este año que buscará tener a su disposición más tecnologías —cámaras de reconocimiento facial y chapas de vehículos, entre otras— que permitan acceder de forma inmediata a información y dentro de un plan de monitoreo de la ciudad¹³. Esto es alarmante porque puede poner en serios riesgos los derechos a la privacidad, libertad de expresión y de reunión y asociación de la ciudadanía paraguaya.

IMPLEMENTACIÓN DE TECNOLOGÍA EN LA TRIPLE FRONTERA

Se identifica un proceso de adopción intensiva de tecnologías en zonas fronterizas del Paraguay, principalmente en las fronteras con Brasil. Concretamente, la Dirección General de Migraciones del Ministerio del Interior se encuentra implementando el Sistema Migratorio Automatizado de Reconocimiento Facial (SMARF), un sistema que captura datos biométricos de reconocimiento facial y que será integrado con la base de datos del Departamento de Identificaciones de la Policía Nacional¹⁴. A dos meses de haberse instalado el sistema, más de 4.000 brasileños y brasileñas lo utilizaron¹⁵.

Se identifica también una tendencia de implementación de tecnologías para fines de seguridad en la ciudad vecina de Foz de Iguazú, en donde destacan una red de drones que sobrevolarán las 24 horas del día la zona de la Triple Frontera, así como la implementación de escáneres de alta precisión para la identificación de chapas de rodados circulando por el

11 «Policía Nacional presentó cámaras corporales que usarán en procedimientos», *La Nación*, 9 de enero de 2021, acceso el 15 de octubre de 2021, <https://www.lanacion.com.py/pais/2021/01/09/policia-nacional-presento-camaras-corporales-que-usaran-en-procedimientos/>

12 «Senado aprueba que agentes usen cámaras corporales en procedimientos», *ADN Digital*, 17 de diciembre de 2020, acceso el 15 de octubre de 2021, <https://www.adndigital.com.py/senado-aprueba-que-agentes-usen-camaras-corporales-en-procedimientos/>

13 «Ministro Arnaldo Giuzzio apostará a la incorporación de más tecnologías en la Policía, en el marco del diseño e implementación de un nuevo modelo de intervención», *Ministerio del Interior*, 23 de enero de 2021, acceso el 15 de octubre de 2021, <http://www.mdi.gov.py/index.php/pnsc/manual-funciones-2020/item/12813-ministro-arnaldo-giuzzio-apostara-a-la-incorporacion-de-mas-tecnologias-en-la-policia-en-el-marco-del-diseño-e-implementación-de-un-nuevo-modelo-de-intervención>

14 «Más de mil personas ya utilizaron el Sistema Migratorio Automatizado de Reconocimiento Facial, en el Puente de la Amistad», *Ministerio del Interior*, 7 de enero de 2021, acceso el 15 de octubre de 2021, <http://www.mdi.gov.py/index.php/pnsc/manual-funciones-2020/item/12778-más-de-mil-personas-ya-utilizaron-el-sistema-migratorio-automatizado-de-reconocimiento-facial-en-el-puente-de-la-amistad>

15 «Sistema de reconocimiento facial en el Puente de la Amistad ya enroló a más de 4.000 personas», *Agencia de Información Paraguaya - IP*, 29 de enero de 2021, acceso el 15 de octubre de 2021, <https://www.ip.gov.py/ip/mas-de-4-000-personas-enroladas-al-sistema-de-reconocimiento-facial-en-el-puente-de-la-amistad/>

Puente de la Amistad¹⁶. El programa, denominado Muralla Inteligente, es una de las ramas de Frontera Tech, vinculado a la Agencia Brasileña de Desarrollo Industrial (ABDI). Frontera Tech ya cuenta actualmente con 70 cámaras con *software* que identifican patrones y generan datos para ayudar al control aduanero y prevenir el contrabando y el tráfico de drogas en el Puente de la Amistad¹⁷.

La adopción de tecnologías de vigilancia que generan un importante caudal de datos personales de carácter sensible y sin las debidas garantías es preocupante y contraria a los estándares internacionales de derechos humanos. A esto se suma una falta de evaluación de impacto de derechos humanos que se repite en la mayoría de las iniciativas tecnológicas por parte del Estado paraguayo.

Por último, la tendencia señalada en el vecino país y la falta de claridad sobre el nivel y grado de compartición de datos e inteligencia entre órganos de seguridad fronteriza¹⁸ dan lugar a una serie de preguntas sobre cómo se comparte este tipo de inteligencia con instituciones paraguayas, qué tipo de acuerdos legitiman dicho intercambio, y qué medidas de seguridad se aplican sobre tales datos. Estas preguntas necesitan ser clarificadas por las fuerzas del orden y seguridad del país involucradas en la materia.

APAGONES DE INTERNET EN LA ZONA NORTE

Según la campaña internacional #KeepItOn de la organización Access Now¹⁹, un apagón de Internet es una interrupción intencional de las comunicaciones electrónicas, que las vuelve inaccesibles o efectivamente inutilizables, para una población específica o dentro de una ubicación, a menudo para ejercer control sobre el flujo de información²⁰. Un apagón de Internet también puede tomar la forma de estrangulamiento, cuando las velocidades de Internet se reducen intencionalmente con el fin de hacer más difícil, o incluso imposible, que las personas suban, descarguen o accedan a información²¹.

16 «Para vigilar la Triple Frontera el Brasil lanza Muralla Inteligente», *Última Hora*, 10 de diciembre de 2020, acceso el 15 de octubre de 2021, <https://www.ultimahora.com/para-vigilar-la-triple-frontera-el-brasil-lanza-muralla-inteligente-n2917861.html>

17 «Muralha inteligente: Itaipu vai investir cerca de R\$ 19 milhões em tecnologia para segurança da fronteira», *Itaipú Binacional*, 7 de diciembre de 2020, acceso el 15 de octubre de 2021, <https://www.itaipu.gov.py/en/node/15215>

18 «Valoran invitación de Brasil al Centro Integrado de Frontera», *La Nación*, 11 de febrero de 2020, acceso el 15 de octubre de 2021, https://www.lanacion.com.py/politica_edicion_impresa/2020/02/11/valoran-invitation-de-brasil-al-centro-integrado-de-frontera/

19 Campaña #KeepItOn de Access Now, <https://www.accessnow.org/keepiton/>

20 Afef Arougui, «Manual sobre apagones de Internet y elecciones», *KeepItOn*, 2021, <https://www.accessnow.org/cms/assets/uploads/2021/06/KeepItOn-Election-and-shutdown-handbook-SPA.pdf>

21 *Ibidem*.

Esto constituye una violación al principio de la neutralidad de la red regulado en territorio paraguayo²².

En ese sentido, el informe de observación de los derechos humanos en la zona norte elaborado por Codehupy da cuenta de graves denuncias por parte de comunidades campesinas de dicho territorio. Concretamente, en su apartado de derechos de asociación, reunión y manifestación, organizaciones sociales y activistas observan que, en los territorios controlados por la Fuerza de Tarea Conjunta (FTC), y previo a operativos liderados por la misma, todos los usuarios de dicha zona se quedan sin cobertura de servicio de telefonía móvil²³. Los testimonios alegan también que ninguna de las líneas de ninguna de las compañías funciona hasta que el operativo de seguridad finalice.

Es vital destacar que la interrupción del acceso a Internet obstaculiza el pleno disfrute de los derechos a la libertad de expresión y opinión, el acceso a la información y la libertad de reunión y asociación. Una declaración conjunta del Relator Especial de las Naciones Unidas (ONU) sobre la libertad de opinión y expresión, la Representante de la Organización para la Seguridad y la Cooperación en Europa (OSCE) sobre la libertad de los medios de comunicación, la Relatora Especial de la Organización de los Estados Americanos (OEA) sobre libertad de expresión, y la Relatora Especial de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP) sobre libertad de expresión y acceso a la información, estableció que cortar o ralentizar el acceso a Internet no se justifica en ningún caso, ni siquiera por razones de orden público o seguridad nacional²⁴.

DATOS PERSONALES: ¿POR QUÉ NOS DEBEN IMPORTAR?

Los datos personales son toda información que se relaciona a una persona física identificada o identificable²⁵. Ejemplo: nombre, apellido, domicilio, fecha de nacimiento, correos electrónicos, número de cédula, dirección de protocolo de Internet IP, número de teléfono, etc. Y está conformada también por los datos sensibles, que son los datos biométricos, genéticos, datos de salud, identidad sexual, convicciones religiosas, afiliaciones sindicales y políticas²⁶.

22 Maricarmen Sequera, «Las continuas violaciones a la neutralidad de la red en Paraguay», *TEDIC*, 5 de abril de 2015, acceso el 15 de octubre de 2021, <https://www.tedic.org/las-continuas-violaciones-a-la-neutralidad-de-la-red-en-paraguay/>

23 Codehupy, *Misión de observación sobre la situación de los derechos humanos en la zona norte* (Asunción: Codehupy, 2021), <https://codehupy.org.py/mision-de-observacion-sobre-la-situacion-de-los-derechos-humanos-en-la-zona-norte/>

24 Frank LaRue et al. (2011), *Joint declaration on freedom of expression and the Internet*, <https://www.osce.org/files/f/ documents/e/9/78309.pdf>

25 Coalición de datos personales (2020), *¿Qué son los datos personales?*, <https://www.datospersonales.org.py/que-son-los-datos-personales/>

26 «¿Qué datos personales se consideran sensibles?», *Comisión Europea*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_es

La doctrina y jurisprudencia de datos personales considera a las afiliaciones políticas dentro de la clasificación de datos sensibles²⁷. Esta clasificación es de gran interés en la regulación específica del tratamiento de este tipo de datos por tener impacto en la vida de las personas. Un mal o abusivo tratamiento de esta información sensible puede generar discriminaciones para el acceso a la salud, a la vivienda, al trabajo, entre otros derechos fundamentales de una persona.

Durante los últimos años, el Partido Colorado realizó afiliaciones compulsivas a su padrón electoral²⁸. Es decir, las hizo sin consentimiento de las personas afectadas²⁹. En el mes de julio de este año hubo una afiliación masiva³⁰ que generó discusiones sobre la importancia de una ley de protección de datos personales y evidenció problemas de ciberseguridad en el sistema del Tribunal Superior de Justicia Electoral y del Registro Cívico Permanente para el resguardo de los datos personales³¹. Como respuesta a esta última afiliación en masa, activistas, abogados y abogadas realizaron durante todo este año acciones de *habeas data* ante el Poder Judicial, para obligar al Partido Colorado a eliminar los datos de las personas que fueron incluidas en su base de datos sin consentimiento expreso. La mayoría de los amparos presentados por la defensa dieron lugar al *habeas data*³². Sin embargo, el Partido Colorado empezó a frenar algunos de ellos por personas influyentes del mismo partido³³, evidenciando serios problemas de independencia judicial.

Por otro lado, los datos relativos a salud son también catalogados como información sensible, y reciben un tratamiento especial por las normativas de protección de datos personales. No cabe duda de que, en un estado de crisis mundial como la generada por el COVID-19, existen ciertas excepciones que pueden llegar a ser aplicables y necesarias, con el fin de preservar la salud y seguridad de la población. Sin embargo, estas injerencias siempre encuentran ciertos límites, y resulta conveniente reflexionar acerca de algunas de

27 Palazzi et al., *Datos personales: Doctrina y jurisprudencia. Tomo 1. Capítulo Protección de Datos. Principios Generales* (Buenos Aires: Editorial CETYS, 2021).

28 Padrón del Partido Colorado, <https://www.anr.org.py/consulta-de-afiliados/>

29 «UNACE promueve amparo constitucional», *Tribunal Superior de Justicia Electoral*, 7 de febrero de 2006, acceso el 15 de octubre de 2021, <https://tsje.gov.py/noticias/leer/75-unace-promueve-amparo-constitucional.html>

30 «Afiliación irregular: Titular de la ANR dice que la web fue hackeada», *Última Hora*, 30 de julio de 2021, acceso el 15 de octubre de 2021, <https://www.ultimahora.com/afiliacion-irregular-titular-la-anr-dice-que-la-web-fue-hackeada-n2953593.html>

31 «ANR ratifica que el Estado ya no puede desentenderse de datos sensibles, afirman», *ABC Color*, 30 de julio de 2021, acceso el 15 de octubre de 2021, <https://www.abc.com.py/nacionales/2021/07/30/caso-anr-ratifica-que-estado-ya-no-puede-desentenderse-de-resguardo-de-datos-sensibles-afirman/>

32 «Justicia obliga a ANR que elimine la afiliación irregular de una ciudadana», *ABC Color*, 24 de abril de 2021, acceso el 15 de octubre de 2021, <https://www.abc.com.py/nacionales/2021/04/24/justicia-ordena-a-la-anr-que-elimine-afiliacion-irregular-de-una-ciudadana/>

33 «Padre de Nenecho frenó un *habeas data* contra la ANR», *Última Hora*, 21 de septiembre de 2021, acceso el 15 de octubre de 2021, <https://www.ultimahora.com/padre-nenecho-freno-un-habeas-data-contra-anr-n2962430.html>

sus implicancias, en especial sobre la publicación de la lista de personas inmunizadas por la vacuna contra el COVID-19³⁴.

Esta lista tiene el fin legítimo de transparentar la agenda de vacunación y evitar la vacunación de personas que no forman parte de los grupos definidos por las políticas públicas del Ministerio de Salud. Sin embargo, el acceso a esta información sensible (personas vacunadas y no vacunadas) por parte de otros actores —como el sector privado, otras instituciones del Estado y personas en general— puede generar discriminaciones al acceso de servicios públicos y privados, impactando a los derechos fundamentales en general.

Esto también se aplica a información sensible de salud. Por ejemplo, la entrega del test de Elisa o examen de VIH fue solicitada por empleadores durante el 2019 y 2020 para acceder a trabajos y generó discriminaciones laborales, traducidas incluso en despidos injustificados³⁵.

Asimismo, el tratamiento de datos personales no es un tema menor en Internet: nuestra vida virtual deja huellas digitales a cada clic en los sistemas de búsqueda, *likes* en las redes sociales, metadatos del contenido³⁶ de una conversación. Con los grandes avances de la industria tecnológica, esta información es almacenada y analizada para predecir el comportamiento y ser vendida como mercancía a otras empresas y grupos de personas y luego vendidos productos y servicios «personalizados». Este modelo de negocios es denominado «capitalismo de vigilancia»³⁷. La regulación a través de las leyes de protección de datos personales es uno de los mecanismos de protección y salvaguarda de las personas en el entorno en línea.

Por todo esto, desde TEDIC, y en conjunto con organizaciones de la sociedad civil, se ha presentado un proyecto de ley de protección de datos³⁸ que está a consideración del Congreso Nacional³⁹. El proyecto es fruto de varios años de trabajo y se basa en recomendaciones internacionales de alto nivel y bien

34 Ley N.º 6794, del 16 de agosto de 2021, «Establece la obligatoriedad de publicar y actualizar en el stock de medicamentos del Ministerio de Salud Pública y Bienestar Social, así como la disponibilidad y registro de vacunaciones contra el COVID-19», *Biblioteca y Archivo Central del Congreso de la Nación*, acceso el 10 de octubre de 2021, <https://www.bacn.gov.py/archivos/9650/LEY%206794.pdf>

35 «La Red de ONGs VIH recibió 51 denuncias por discriminación laboral», *La Nación*, 5 de mayo de 2021, acceso el 15 de octubre de 2021, <https://www.lanacion.com.py/pais/2021/05/05/la-red-de-ongs-vih-recibio-51-denuncias-por-discriminacion-laboral/>

36 Los metadatos son datos sobre los datos. Es decir, describen el contenido de los archivos o la información de los mismos.

37 Rob Lucas, «Capitalismo de Vigilancia», *NUSO* N.º 290 - Noviembre-Diciembre 2020, <https://nuso.org/articulo/capitalismo-de-vigilancia/>

38 «El Congreso da entrada oficial al proyecto de ley de protección de datos personales», *TEDIC*, 4 de mayo de 2021, acceso el 15 de octubre de 2021, <https://www.tedic.org/el-congreso-nacional-da-entrada-oficial-al-proyecto-de-ley-de-proteccion-de-datos-personales/>

39 «Ficha Técnica del Expediente», *SilPy - Sistema de Información Legislativa*, acceso el 15 de octubre de 2021, <http://silpy.congreso.gov.py/expediente/123459>

documentadas⁴⁰. De aprobarse, otorgará a las personas el derecho a elegir libremente en qué circunstancias y en qué medida expondrán información sobre sí mismas, y les permitirá realizar acciones legales en situaciones de abuso, violaciones y arbitrariedades sobre sus datos personales⁴¹.

EXPLORANDO NUEVAS MODALIDADES DE TRABAJO EN EL ÁMBITO DIGITAL

La Ley N.º 6738/2021 «Que establece la modalidad de teletrabajo en relación de dependencia» determina una serie de criterios y salvaguardas que permiten a trabajadores y trabajadoras de los sectores público y privado la posibilidad de trabajar a distancia⁴². La misma se encuentra actualmente en proceso de reglamentación a cargo del Ministerio de Empleo, Trabajo y Seguridad Social (MTESS)⁴³. TEDIC destaca la relevancia de que los poderes Ejecutivo y Legislativo discutan sobre estas recientes modalidades laborales, dando posibilidad a nuevos formatos de trabajo.

Particularmente, resalta como positivo el reconocimiento del derecho a la desconexión como una garantía expresa en la ley. Se obliga así a que empleadores(as) respeten el derecho de la persona trabajadora a desconectarse por lo menos doce horas continuas, aclarando que no está obligada a responder comunicaciones, órdenes u otros requerimientos⁴⁴. Dicho esto, es importante reflexionar sobre algunos problemas planteados en la ley, que pueden comprometer el espacio íntimo y la privacidad de las personas teletrabajadoras.

En su artículo 19, esta norma establece la posibilidad de que el empleador o la empleadora realice visitas al domicilio de la persona teletrabajadora para controlar el cumplimiento de las normas de salud y seguridad ocupacional, así como para el mantenimiento de los equipos informáticos⁴⁵. Esto es problemático pues, dependiendo del caso, pueden existir personas teletrabajadoras que no deseen este tipo de visitas por cuestiones no relacionadas con el ámbito laboral, y que responden más bien a particularidades de su familia, su ubicación geográfica y un sinnúmero de posibilidades que las mismas tienen derecho a resguardar, si así lo desean.

40 Coalición de datos personales de la sociedad civil y empresas, <https://www.datospersonales.org.py/>

41 Nekane Alonso, «Autodeterminación informativa», *Grupo Ático*34, 29 de septiembre de 2020, acceso el 15 de octubre de 2021, <https://protecciondatos-lopd.com/empresas/autodeterminacion-informativa/>

42 Ley N.º 6738/2021, del 24 de mayo de 2021, «Que establece la modalidad de teletrabajo en relación de dependencia», *Congreso Nacional*, acceso el 15 de octubre de 2021, https://www.mtess.gov.py/application/files/6016/2265/4905/Ley_N_6738-21_Modalidad_de_Teletrabajo_en_relacion_de_dependencia.pdf

43 «El teletrabajo ya es ley en Paraguay y su reglamentación está a cargo del MTESS para el sector privado», *Ministerio de Trabajo, Empleo y Seguridad Social*, 2 de junio de 2021, acceso el 15 de octubre de 2021, <https://www.mtess.gov.py/noticias/el-teletrabajo-ya-es-ley-en-paraguay-y-su-reglamentacion-esta-cargo-del-mtess-para-el-sector-privado>

44 *Ibidem* 42.

45 *Ibidem*.

Por último, un fenómeno en alza —que no ha recibido mucha atención por parte de hacedores de políticas públicas— es el creciente número de personas trabajadoras de «economía de plataforma» desarrollada en el país. Dicha economía se caracteriza por la independencia y contingencia de las actividades que realizan sus personas trabajadoras y en donde la oferta y la demanda laboral se organizan a través de una infraestructura digital y algorítmica⁴⁶. La supervisión de este fenómeno por parte de algunas instituciones públicas ha demostrado ser, en el mejor de los casos, aislada entre diferentes entes gubernamentales y municipales. En el peor de los casos, ha sido insuficiente y sin un enfoque basado en el bienestar de las y los trabajadores. Predomina una perspectiva de análisis desde el derecho a la competencia y regulación del transporte y sin incorporar una perspectiva de derechos humanos⁴⁷.

VIOLENCIA DIGITAL DE GÉNERO

Durante la pandemia del COVID-19, la violencia contra las mujeres se ha manifestado de diversas formas, incluidas la violencia doméstica y la violencia en línea. Las consecuencias y los daños causados por las diferentes manifestaciones de la violencia en línea guardan una estrecha relación con el género: las mujeres, las niñas y adolescentes sufren un estigma particular en un contexto de desigualdad estructural y discriminación.

Este año, en el marco de las acciones sobre género y tecnología, TEDIC ha publicado dos investigaciones: una sobre la violencia digital de género⁴⁸ y otra referida a la difusión de imagen íntima no consentida⁴⁹. Ambos estudios exploratorios exponen la ausencia de políticas públicas para mitigar la violencia que afecta a mujeres, niñas, comunidad LGTBQI+, comunidades campesinas e indígenas que acceden a Internet. Los hallazgos se centran en las barreras de acceso a la justicia ejemplificadas en la falta de respuesta efectiva y rápida por parte del Estado. El enfoque de las defensas y resoluciones judiciales se basa en la protección de la reputación y el honor, y no en el derecho y las libertades. Existe poca o insuficiente argumentación con enfoque de género, revictimizando a la persona que decide realizar una denuncia.

- **Difusión de imagen no consentida.** Las resoluciones del Poder Judicial siguen reproduciendo argumentos conservadores y patriarcales para proteger a la víctima de violencia digital. Entre otras expresiones, se usa

46 Arturo Arriagada et al., «Fairwork Chile Ratings 2021: Labour Standards in the Platform Economy», *FairWork*, 2021, acceso el 15 de octubre de 2021, <https://fairwork/en/fw/publications/fairwork-chile-puntuaciones-2021/>

47 Eduardo Carrillo, «Apps de transporte y regulación de la competencia en Paraguay», *TEDIC*, 29 de enero de 2021, acceso el 15 de octubre de 2021, <https://www.tedic.org/apps-de-transporte-y-regulacion-de-la-competencia-en-paraguay/>

48 Maricarmen Sequera, *Difusión de imagen íntima no consentida - Un estudio exploratorio* (Asunción: TEDIC, 2021), <https://www.tedic.org/wp-content/uploads/2021/09/Imagen-no-consentida-Tedic-web.pdf>

49 Diana García y Maricarmen Sequera, *Violencia de género en Internet en Paraguay - Un estudio exploratorio* (Asunción: TEDIC, 2021), <https://www.tedic.org/wp-content/uploads/2021/08/Violencia-Digital-TEDIC-WRO-2021-ES-v01.pdf>

«persona de bien», «mujeres de familia», «actividades de carácter inmoral», para describir el daño a la imagen en los casos de difusión de imagen íntima no consentida. Por otro lado, se evidenció la falta de datos desagregados en el sistema judicial, que impide analizar la violencia digital de género y abordar el problema con mayor eficiencia y eficacia desde el Estado.

- **Violencia de género en Internet en Paraguay.** Todas las mujeres entrevistadas y encuestadas reconocieron haber recibido violencia digital por lo menos una vez en su vida. Entre los hallazgos de este estudio se encontraron: la falta de identificación de los tipos de violencia digital por parte de las víctimas y la comunidad; la negación de la víctima de violencia digital y la minimización de la violencia digital como una violencia menor o inexistente por parte de la víctima, la comunidad y la justicia. Por ejemplo, las mujeres políticas que tienen una vida activa y pública en Internet consideran que, más que violencia digital de género, este tipo de «situaciones» son un «derecho a piso» que deben pagar. Las mujeres del área rural también reciben acoso que empieza en Internet, se traslada a mensajes SMS de telefonía y luego a acoso callejero. Esto no es muy diferente a la violencia digital que sufren las de áreas urbanas: gran parte de la violencia se concentra en lo digital, pero también se traslada al mundo físico. Asimismo, las violencias son perpetradas mayoritariamente por personas cercanas: pareja o expareja o pertenece al círculo inmediato —miembros de la familia, compañeros de trabajo o amigos— y, en un segundo plano, por desconocidos (anónimos).

CONCLUSIONES

Se observa una tendencia ya documentada en años anteriores, que da cuenta de la falta de un enfoque de derechos humanos a la hora de adoptar tecnologías para la implementación de políticas públicas. Esta ausencia tiene un impacto en el pleno disfrute de los derechos humanos de la ciudadanía paraguaya, con un particular efecto desproporcionado en comunidades vulnerables.

La recolección intensiva de datos biométricos a través de los sistemas AFIS y SMARF, así como la posible integración entre bases de datos con distintos fines y naturalezas, abre un abanico de posibles abusos por parte de autoridades públicas que podrían impactar negativamente en el disfrute de los derechos humanos de las personas. También es importante preguntarse sobre la propiedad de estos sistemas informáticos adquiridos por el Gobierno y acerca de qué tipo de garantías son establecidas para salvaguardar la soberanía digital y de datos personales de la población.

Por otra parte, las graves denuncias de comunidades asentadas en el norte sobre un posible escenario de apagones de Internet en momentos previos a un operativo militar de la FTC son un grave retroceso de la institucionalidad paraguaya y los compromisos internacionales asumidos por el Estado paraguayo en materia de derechos humanos.

El aumento del tratamiento de los datos personales en bases de datos sin un marco regulatorio en el país puede poner riesgo al acceso de las personas a otros derechos fundamentales, como a la privacidad, la libertad de expresión, el derecho a la salud, a la información, el derecho al trabajo, entre otros. Al cierre de este informe, el proyecto de ley de protección de datos personales se encuentra en el Congreso Nacional. El reto del Estado es garantizar la protección y la seguridad de las personas en el entorno digital.

Así también, la tendencia de digitalización de procesos laborales requiere una respuesta coordinada y de múltiples partes interesadas, que asegure el pleno respeto y la protección de los derechos laborales ya establecidos en la legislación paraguaya. De lo contrario, se corre el peligro de que —bajo una interfaz digital que apunta a enmascarar situaciones como el *rankeo* de trabajadores(as) a través de algoritmos no transparentes o políticas que no permiten la organización sindical— trabajadoras y trabajadores se expongan a nuevos tipos de abusos.

Por último, y en lo que respecta a la violencia digital de género, el gran desafío es comprender a la violencia digital contra la mujer como un continuo de la violencia que sufren las mujeres «fuera de línea». Este fenómeno no debe ser considerado distinto, sino tiene que ser incluido como una extensión de la violencia a través de la tecnología. En ese sentido, las normativas y políticas públicas en el país no cuentan con una armonización que considere la violencia digital como una extensión de la violencia física. Esta falta de consideración conlleva la invisibilización y desprotección de las mujeres en el entorno digital. El Estado paraguayo no realiza estudios ni puntos de referencia que profundicen y reconozcan el problema en el país. Aún no se evidencia capacidad institucional para generar políticas públicas basadas en evidencias y así salvaguardar, proteger y reparar a las mujeres, niñas y adolescentes de esta violencia de manera integral.

RECOMENDACIONES

- Suspender la recolección masiva de datos a través de AFIS y SMARF, hasta tanto no se realicen evaluaciones de su impacto relacionadas a los derechos humanos. Estos estudios deben contemplar los principios de necesidad y proporcionalidad, a través de los cuales se determinará si estos sistemas son adecuados para su propósito.

- Sancionar con urgencia en el Poder Legislativo el proyecto de ley de protección integral de datos personales en Paraguay. Este marco legal regulará los tratamientos de datos personales y evitará abusos y arbitrariedades en la vida de las personas.
- Conformar un equipo integrado por autoridades públicas y de la sociedad civil para investigar debidamente las denuncias de apagones de Internet y, en caso de que las mismas sean confirmadas, sancionar a los actores públicos y privados involucrados.
- Facilitar un proceso de reglamentación de la Ley N.º 6738/2021 que priorice el resguardo de la privacidad de las personas teletrabajadoras, y que ofrezca la posibilidad de elección a la hora de permitir las inspecciones de empleadores(as) en su espacio íntimo. Importante es, además, que este proceso de reglamentación incorpore salvaguardas para mujeres trabajadoras víctimas de violencia doméstica y que considere también la sobrecarga en las tareas de cuidado absorbida por ellas.
- Generar regulaciones robustas que protejan el principio de neutralidad en la red, que aborden de manera integral el acceso a Internet sin discriminación y que no se generen «parches legales» que afecten negativamente el acceso a una Internet de calidad. Censurar el acceso a Internet a través de bloqueos es una forma de violentar los derechos fundamentales en el entorno en línea.
- Reconocer a la violencia de género en línea como una violación a los derechos humanos y como un *continuum* de las agresiones que viven las mujeres en espacios físicos, que se complejizan y se amplían a través del uso de la tecnología.
- Crear políticas públicas basadas en evidencia, con la realización de un diagnóstico sobre la brecha digital de género que incluya divisiones tales como: zonas urbanas y rurales, rango etario, mujeres, hombres y otros, franja de ingresos y clase social, nivel educativo, nivel de alfabetización, grados de uso, tipos de dispositivos, ancho de banda, precios, etc. La eficacia de las políticas públicas e inclusive los planes de negocios de las empresas deben considerar esta información clave para adoptar medidas integrales, a fin de mitigar la violencia de género de acuerdo con los Objetivos y Metas de Desarrollo Sostenible (ODS).

