DERECHOS DIGITALES

Entre la conectividad y la exclusión: asignaturas pendientes en Paraguay

El 2025 expone un dilema: Paraguay avanza en protección de datos, pero permanece vulnerable ante la vigilancia estatal, la violencia digital y las tecnologías sin regulación. Los derechos digitales siguen en disputa en un entorno donde la innovación supera a las garantías, y la ciudadanía continúa enfrentando riesgos que comprometen su privacidad, su seguridad y su participación en la vida pública.

Palabras claves: *derechos digitales, protección de datos personales, ciberseguridad, vigilancia, inteligencia artificial.*

Jazmín Ruiz Díaz Figueredo
TEDIC

En este artículo se abordará la situación de los derechos digitales en Paraguay durante el 2025, la cual expone un dilema entre la conectividad y la exclusión. El análisis se centra en cómo el país, a pesar de los avances institucionales, como la sanción del proyecto de Ley de Protección de Datos Personales, permanece vulnerable ante la vigilancia estatal, la violencia digital y las tecnologías sin regulación. El foco está puesto en varios desafíos pendientes. En primer lugar, se abordará el panorama legislativo de ciberseguridad, donde las iniciativas se presentan de forma fragmentada y apresurada, con una orientación excesivamente securitaria y centralizada que amenaza con convertir la ciberseguridad en una herramienta de control estatal y vigilancia masiva. A continuación se exponen graves incidentes de vulneración de derechos por parte del Estado, incluyendo el espionaje digital ilegal a manifestantes de la «Generación Z» y el uso no regulado de tecnologías biométricas —como el reconocimiento facial— en espacios como la Expo Paraguay 2025, lo que plantea riesgos de exclusión y concentración de datos sensibles. La tercera dimensión de este informe cubre la necesidad urgente de una gobernanza tecnológica centrada en los derechos humanos y la transparencia, especialmente ante el uso de la inteligencia artificial, que carece de una estrategia nacional y marcos éticos claros.

SITUACIÓN DEL DERECHO EN 2025

AVANCES INSTITUCIONALES Y DESAFÍOS PENDIENTES

La evolución tecnológica ha abierto nuevas oportunidades para el ejercicio de la libertad de expresión, el acceso a la información y la participación ciudadana. Sin embargo, también ha amplificado riesgos y amenazas existentes, como la violencia de género facilitada por la tecnología y la desinformación, que ponen en peligro el ejercicio pleno de los derechos humanos y atentan contra la integridad de los procesos democráticos. De allí que hablamos de la importancia de los derechos digitales como una extensión de los derechos humanos. Al igual que en el mundo físico, estos derechos se encuentran en constante disputa y pueden ser vulnerados.

En el Paraguay, aunque la Constitución reconoce garantías fundamentales y existe legislación aplicable, persisten vacíos normativos y desafíos en su implementación. En ese sentido, al cierre de este informe, se celebraba la reciente sanción del proyecto de ley en la Cámara de Senadores y se esperaba su promulgación por parte del Poder Ejecutivo[1]. Esta ley reconoce que los datos personales pertenecen a las personas y que su uso debe regirse por los principios de consentimiento, transparencia y responsabilidad.

1 «Ficha Técnica del Expediente #2162170», *SILPy - Sistema de Información Legislativa*, acceso el 10 de octubre de 2025, https://bit.ly/3JLbgjP

Supone, por lo tanto, un cambio de enfoque: desplaza la atención de la información como un bien meramente técnico para colocar en el centro a las personas a quienes esa información representa.

Sobre este punto, Maricarmen Sequera[2], como directora ejecutiva de TEDIC, destaca:

> Después de nueve años de trabajo constante de la Coalición de Datos Personales[3] para instalar este tema en la agenda pública y cuatro años de incidencia sostenida en el ámbito legislativo, hoy vemos concretado un paso fundamental hacia la protección integral de los derechos digitales en nuestro país.

Además, el Congreso impulsó varias propuestas legislativas orientadas a regular la ciberseguridad, los ciberdelitos y la protección de datos personales.

Iniciativas legislativas

A fines de mayo de 2025, se presentaron dos propuestas en la Cámara de Diputados y un anteproyecto:

1. Proyecto de Ley «De Ciberseguridad, Protección de Datos y Prevención de Ciberdelitos», presentado por el diputado Germán Solinger[4], ingresado el 12 de mayo de 2025.

2. Proyecto de Ley «De Ciberseguridad y Protección del Ciberespacio Paraguayo», del diputado Luis Federico Franco Alfaro[5], ingresado el 28 mayo de 2025.

3. Anteproyecto de Ley de Ciberseguridad, liderado por la Universidad Metropolitana de Asunción[6], acompañado por una audiencia pública, que abre la puerta a una conversación más amplia.

Sin embargo, Sequera[7] advierte que las iniciativas legislativas fueron elaboradas de manera fragmentada y apresurada, sin una articulación adecuada entre las distintas áreas jurídicas. Se observa una tendencia a mezclar conceptos y competencias de ciberseguridad, ciberdelito y protección de datos, lo que genera confusión normativa y debilita la efectividad de las políticas públicas.

---

2 Maricarmen Sequera en conversación electrónica con la autora el 5 de noviembre de 2025.

3 La Coalición de Datos Personales está conformada por TEDIC, APADIT, PUENTE e Internet Society, capítulo Paraguay.

4 «Ficha Técnica del Expediente #2584479», *SILPy - Sistema de Información Legislativa*, acceso el 10 de octubre de 2025, https://bit.ly/4rfXdDQ

5 «Ficha Técnica del Expediente #2584815», *SILPy - Sistema de Información Legislativa*, acceso el 10 de octubre de 2025, https://bit.ly/3MonqG2

6 Anteproyecto https://bit.ly/4pc4faP

7 Maricarmen Sequera Buzarquis, «Ciberseguridad en Paraguay: entre la urgencia y la improvisación legislativa», *TEDIC*, 23 de junio de 2025, acceso el 20 de octubre de 2025, https://bit.ly/3XvlS9C

También critica la falta de técnica legislativa —objetos de ley mal definidos, glosarios imprecisos y escasa fundamentación técnica—, así como la orientación excesivamente securitaria y centralizada en actores policiales o militares. Este enfoque podría desplazar el protagonismo de organismos civiles y debilitar las garantías de derechos humanos en el entorno digital. Desde su análisis, plantea que una política pública de ciberseguridad debe construirse desde un enfoque de derechos, participación multisectorial y transparencia, incorporando principios técnicos, como el cifrado de extremo a extremo, la privacidad por diseño y la rendición de cuentas institucional. Asimismo, subraya la importancia de que cualquier normativa se alinee con estándares internacionales de gobernanza democrática de la tecnología.

El panorama descrito revela el riesgo de que la legislación sobre ciberseguridad, en lugar de fortalecer la protección ciudadana, se convierta en una herramienta de control estatal y vigilancia masiva. Esto representa una potencial vulneración de los derechos a la privacidad, la libertad de expresión y la participación pública. La improvisación normativa, sumada a la ausencia de mecanismos de supervisión independientes, amenaza con consolidar un modelo de ciberseguridad orientado a la represión y no a la protección integral de las personas usuarias. Entendiendo que una «ciberseguridad verdaderamente democrática no solo bloquea amenazas: también habilita libertades, crea confianza y reduce las desigualdades. Y, sobre todo, no criminaliza a quienes participan del mundo digital, sino que los acompaña, los cuida y los empodera»[8].

Estrategia Nacional de Ciberseguridad 2025-2028

Por otra parte, un paso decisivo que se dio en 2025 hacia la consolidación de una política nacional de ciberseguridad ha sido la aprobación de la Estrategia Nacional de Ciberseguridad 2025-2028, mediante el Decreto N.º 3900/25[9]. Este nuevo marco reemplaza al Plan de 2017 e introduce una estructura institucional robusta, encabezada por la Dirección General de Ciberseguridad y Protección de la Información (DGCPI) y el Centro de Respuestas a Incidentes Cibernéticos del Paraguay (CERT-PY), como órgano operativo ante incidentes. La estrategia busca superar deficiencias históricas relacionadas con la falta de coordinación, métricas y formación, incorporando programas de capacitación, cooperación internacional y reformas legales orientadas a la resiliencia digital.

8 «La Evolución de la Ciberseguridad en Paraguay: MITIC como Pilar Estratégico», *TEDIC*, 24 de junio de 2025, acceso el 20 de octubre de 2025, https://bit.ly/48dNd6h

9 Decreto N.º 3900/25, en «Estrategia Nacional de Ciberseguridad 2025-2028», *CERT-PY*, acceso el 10 de octubre de 2025, https://bit.ly/4pc4YZB

El proceso de elaboración, liderado por el Ministerio de Tecnologías de la Información y Comunicación (MITIC), con apoyo de la Organización de los Estados Americanos (OEA), contó con la participación de más de 250 actores del sector público y privado. Sin embargo, TEDIC[10] observó que varios aportes de la sociedad civil no fueron incorporados en la versión final. Entre sus críticas destacan: la ausencia de una gobernanza inclusiva con enfoque de derechos, la falta de mecanismos de participación multisectorial y un énfasis punitivo por encima del enfoque preventivo. Según la organización, una ciberseguridad democrática debe incluir a instituciones como los ministerios de Salud, Mujer y Niñez, así como priorizar la educación digital, la prevención de la violencia en línea y la protección de colectivos vulnerables. Además, enfatiza que la ciberseguridad «no puede construirse sin cuidado, ni puede funcionar sin empatía», pues exige «una transformación profunda que coloque en el centro a la dignidad humana, los derechos digitales y la justicia social»[11].

INTELIGENCIA ARTIFICIAL: ENTRE VACÍOS LEGALES Y PREGUNTAS ÉTICAS ABIERTAS

Durante el periodo analizado, el debate sobre la regulación de la inteligencia artificial (IA) en Paraguay evidenció avances iniciales, aunque el proceso legislativo mantuvo como prioridad la aprobación de la Ley de Protección de Datos Personales, reconocida como una condición necesaria para garantizar la protección de derechos fundamentales en el entorno digital. En una audiencia pública organizada por la Comisión de Ciencias, Tecnología, Innovación y Futuro del Congreso Nacional, distintos actores del sector público, privado y de la sociedad civil —incluyendo al MITIC, la Corte Suprema de Justicia (CSJ), la Policía Nacional (PN) y la Sociedad Paraguaya de Inteligencia Artificial (Sopaia)— abordaron los alcances y riesgos asociados a la implementación de sistemas de IA[12].

El intercambio permitió identificar una preocupación transversal respecto a la necesidad de contar con un marco normativo que incorpore salvaguardas adecuadas en materia de privacidad, transparencia, rendición de cuentas y no discriminación algorítmica. En este sentido, el énfasis legislativo en la protección de datos personales fue interpretado como un paso preliminar hacia la construcción de una gobernanza tecnológica basada en derechos humanos. Asimismo, se destacó la relevancia de fortalecer la ciberseguridad y la alfabetización digital de la población como componentes esenciales para reducir las brechas de acceso, prevenir vulneraciones y promover un uso ético y seguro de las tecnologías emergentes.

10 *Ibidem*.

11 *Ibidem*.

12 «Socializan proyecto que regula el desarrollo e implementación de la IA», *Cámara de Senadores*, 26 de junio de 2025, acceso el 10 de octubre de 2025, https://bit.ly/3WZOJmj

Más allá del anteproyecto de ley, cuando se examinan el crecimiento y las implicaciones de la inteligencia artificial (IA) en Paraguay, uno de los puntos que se destacan es el potencial del país para albergar centros de datos debido a su energía hidroeléctrica[13]. Sin embargo, a pesar del interés internacional y las conversaciones para construir un gran centro de datos, el uso de la IA por parte del Gobierno y las empresas carece de una estrategia nacional coherente y se limita a esfuerzos aislados, principalmente en la Dirección Nacional de Contrataciones Públicas (DNCP). Expertas de instituciones como MITIC, TEDIC y Sopaia[14] identifican graves riesgos por la falta de un marco regulatorio, incluyendo la pérdida de soberanía por la entrega de datos estatales a servicios extranjeros y el potencial de la IA para exacerbar las desigualdades sociales debido a sesgos algorítmicos entrenados en el norte global. El riesgo de la pérdida masiva de empleo, la desregulación del reconocimiento facial y el aumento de la desinformación son preocupaciones centrales para la democracia y la seguridad ciudadana, si no se implementan legislaciones de protección de datos. Si bien se discuten modelos como el de Chile para una IA proactiva, la conclusión es que Paraguay necesita una mayor alfabetización digital y construir una IA que esté al servicio de las personas y no al revés.

CASOS OCURRIDOS EN 2025

CIBERATAQUES A LA FRONTERA DIGITAL

En mayo de 2025, un ataque cibernético coordinado afectó los sitios web de más de diez entidades estatales, entre ellas la Presidencia, la Cámara de Diputados y el Ministerio de Salud, con el propósito de sustraer datos sensibles[15]. Asimismo, se registró la usurpación de la identidad digital del presidente Santiago Peña en la red social X[16], evidenciando la exposición de las autoridades nacionales ante amenazas de este tipo. A esto se suma la alta frecuencia de ataques menos sofisticados: solo en abril de 2025 se reportaron cerca de 200 incidentes en el país, ejecutados mediante herramientas de bajo costo como *malware* y *phishing*[17], lo que refuerza la percepción de debilidad en las defensas digitales paraguayas.

13 Norma Flores Allende, «¿Qué tan protegidos estamos en la era de la IA en Paraguay?», *The Paraguay Post*, 15 de octubre de 2025, acceso el 10 de octubre de 2025, https://bit.ly/44ds0Hh

14 *Ibidem*.

15 «Paraguay sufrió un "ataque cibernético coordinado"», *Página* 12, 13 de mayo de 2025, acceso el 20 de octubre de 2025, https://bit.ly/40Bxsfn

16 «Investigan posible hackeo a la cuenta de X del presidente de la República», *La Nación*, 9 de junio de 2025, acceso el 20 de octubre de 2025, https://bit.ly/3LGU8w6

17 «Informe de Ciberseguridad Abril 2025. Incidentes reportados (Spam, Malware, Phishing, entre otros)», *Observatorio de Innovación de Paraguay*, https://bit.ly/4p9S7Hb

A septiembre de 2025, suman 47 los ciberataques a los sistemas del Gobierno Nacional. Los incidentes de ciberespionaje e intrusión que mejor ilustran la vulnerabilidad digital paraguaya se dividen en dos categorías principales: ciberespionaje estatal estratégico y ataques disruptivos masivos, las cuales han afectado instituciones como la Cancillería paraguaya y la hidroeléctrica Itaipú[18].

Estos incidentes de ciberataques estatales subrayan la vulnerabilidad de Paraguay frente a actores más sofisticados, demostrando que la información vinculada con la política exterior, la infraestructura crítica y los intereses económicos estratégicos constituyen un blanco constante.

PROTESTA DE LA «GENERACIÓN Z»

El 28 de septiembre de 2025, jóvenes autodenominados «Generación Z» organizaron una manifestación en Asunción para protestar contra la corrupción. Según reportes[19], la Policía Nacional, a través de su Departamento de Cibercrimen, llevó a cabo una operación de espionaje digital previo al evento, infiltrándose en grupos de WhatsApp, Telegram y otras redes sociales utilizadas por las personas organizadoras. Los agentes implicados, entre comisarios y oficiales, justificaron su acción como un mecanismo preventivo ante la sospecha de que las personas organizadoras planeaban «incitación a cometer hechos punibles y apología del delito»[20]. Sin embargo, expertos y observadores han cuestionado la legalidad de este monitoreo: el abogado penalista Juan Pablo Irrazábal sostuvo que el Estado no puede ingresar a «espacios que se asumen como fuentes abiertas» sin autorización judicial, porque se trata de una vulneración de la privacidad[21]. Por su parte, Maricarmen Sequera, de TEDIC, advirtió sobre una «vigilancia ilegal», dado que no existía hasta ese momento una conducta delictiva comprobada[22].

Tras la movilización, 31 personas fueron detenidas y trasladadas a la Agrupación Especializada. Horas más tarde, la Fiscalía informó que no pudo acreditar hechos punibles concretos contra las personas manifestantes. Legisladores también recogieron los testimonios de las personas detenidas en una sesión de la Cámara de Diputados sobre derechos humanos[23].

18 Julieta H. Heduvan, «Paraguay en el ciberespacio: Vulnerabilidades estratégicas en la frontera digital», *TEDIC*, 29 de agosto de 2025, acceso el 20 de octubre de 2025, https://bit.ly/4i0pbz3

19 «Así espió la Policía a los jóvenes que organizaron la manifestación de la Generación Z», *Última Hora*, 30 de septiembre de 2025, acceso el 20 de octubre de 2025, https://bit.ly/3LKetk8

20 *Ibidem*.

21 «Abogado critica a la Policía por espiar en redes a la Gen Z: "El Estado no puede hacer eso"», *Última Hora*, 1 de octubre de 2025, acceso el 20 de octubre de 2025, https://bit.ly/4i6UUik

22 «Espionaje en redes de la Gen Z: Tedic advierte sobre "vigilancia ilegal" de la Policía», *Última Hora*, 1 de octubre de 2025, acceso el 20 de octubre de 2025, https://bit.ly/44272Lq

23 «Escuchan testimonios de jóvenes detenidos durante movilización de la "Generación Z"», *Honorable Cámara de Diputados*, 13 de octubre de 2025, acceso el 20 de octubre de 2025, https://bit.ly/3WTXzlB

Este caso constituye una vulneración del derecho a la privacidad, que garantiza que las interacciones en línea (mensajería, grupos, redes) no sean monitoreadas arbitrariamente por el Estado sin una justificación legal adecuada. Además, atenta contra el derecho a la libre expresión y asociación, ya que la vigilancia preventiva disuade la organización de protestas y puede tener un efecto inhibidor sobre la libre reunión y la expresión de ideas en espacios digitales y físicos. Finalmente, es un ataque al derecho a la libertad de manifestación: si la Policía monitoriza digitalmente a las personas organizadoras, limita su capacidad de planificar y ejercer su derecho a protestar, lo que puede ser una forma de represión informática.

USO DE TECNOLOGÍAS BIOMÉTRICAS EN LA EXPO

En julio de 2025 se llevó a cabo una nueva edición de la Expo Paraguay, organizada por la Asociación Rural del Paraguay (ARP) y la Universidad Rural del Paraguay (URP). Este evento, de alto impacto económico y social, reunió a diversos sectores de la agroindustria y otros rubros productivos. Sin embargo, la edición de 2025 estuvo marcada por cuestionamientos relacionados con el uso de tecnologías de acceso basadas en datos biométricos y sistemas digitales de pago, los cuales generaron preocupaciones significativas en materia de inclusión, privacidad y protección de datos personales[24].

Para ingresar al predio ferial, las personas asistentes debían utilizar obligatoriamente la aplicación Tutti y efectuar los pagos a una cuenta del banco digital Ueno Bank, además de someterse a un proceso de verificación biométrica —mediante reconocimiento facial o huella dactilar—, gestionado por la empresa ITTI. Las tres entidades forman parte de un mismo grupo económico, lo que concentró en un solo actor privado la recolección y el procesamiento de datos financieros y biométricos de miles de personas. Este modelo generó exclusión hacia sectores no bancarizados, personas mayores y usuarios sin acceso o conocimiento tecnológico, al tiempo que planteó riesgos graves para la protección de datos sensibles.

Diversas voces del ámbito político y social señalaron que la implementación de este sistema de acceso careció de criterios de equidad, transparencia y garantías de derechos fundamentales[25]. La ausencia de mecanismos de supervisión o auditoría sobre el tratamiento de los datos biométricos recopilados —incluyendo su almacenamiento, uso y eventual eliminación— acentuó las preocupaciones sobre posibles vulneraciones al derecho a la privacidad, la libertad de circulación y la no discriminación.

24 «Expo Paraguay 2025: vigilancia, desprotección y exclusión a la ciudadanía», *TEDIC*, 23 de julio de 2025, acceso el 20 de octubre de 2025, https://bit.ly/3XsKy2v

25 *Ibidem*.

El caso de la Expo Paraguay 2025 puso en evidencia una tendencia creciente en el país: la adopción de tecnologías de reconocimiento facial y otros sistemas de vigilancia biométrica sin un marco regulatorio específico. Actualmente, estas tecnologías se están implementando en espacios públicos, estadios, instituciones estatales y edificios privados, en un contexto de opacidad institucional y ausencia de controles ciudadanos. Organizaciones como TEDIC[26] han documentado que estas prácticas se desarrollan sin garantías de transparencia ni evaluación de impacto en derechos humanos, y que en algunos casos podrían estar asociadas a un uso indebido de fondos públicos.

La recopilación y el tratamiento de datos biométricos —tales como huellas dactilares, rostros, iris, voz o patrones de movimiento— implican un nivel de riesgo especialmente alto, dado que estos datos son únicos e irremplazables. En situaciones de vulneración o filtración, las consecuencias pueden ser irreversibles y propiciar suplantación de identidad, fraudes o vigilancia no autorizada. Estos antecedentes refuerzan la necesidad urgente de contar con una Ley de Protección de Datos Personales robusta, que establezca principios de minimización, consentimiento informado, proporcionalidad, finalidad legítima y transparencia en el tratamiento de información personal.

La situación observada en la Expo Paraguay 2025 ilustra de manera concreta los desafíos que enfrenta el país en materia de derechos digitales. La falta de regulación específica y de controles efectivos sobre el uso de tecnologías biométricas pone en riesgo derechos fundamentales y profundiza las desigualdades en el acceso a servicios y espacios públicos. En este contexto, resulta imperativo que el Estado paraguayo adopte medidas urgentes para garantizar la transparencia, la rendición de cuentas y el respeto de los derechos humanos en el uso de tecnologías emergentes.

El monitoreo continuo, la educación digital ciudadana y la pronta aprobación de un marco legal de protección de datos personales son pasos indispensables para consolidar una gobernanza tecnológica basada en derechos, donde la innovación se desarrolle de manera ética, inclusiva y respetuosa de la dignidad humana.

26 *Ibidem.*

LEY «NO MOLESTAR»: LECCIONES DEL CASO CLARO VERSUS SEDECO

El caso Claro contra la Secretaría de Defensa del Consumidor y el Usuario (SEDECO)[27] constituye un hito judicial en Paraguay, con un impacto significativo en la legislación sobre privacidad y derechos digitales. Esta decisión reafirmó el poder de los consumidores, evidenció las limitaciones estructurales del marco normativo vigente y generó impulso hacia reformas urgentes.

La sentencia —emitida en diciembre de 2024 y que ratificó una sanción contra la empresa de telecomunicaciones AMX Paraguay S.A. (Claro) por contactar a usuarios inscritos en el listado de exclusión publicitaria[28]— ofrece una lectura actualizada y valiosa desde una perspectiva de derechos humanos. Un estudio del caso[29] subraya la fragmentación de la normativa paraguaya y considera que la Ley N.º 5830/17 «No Molestar» resulta insuficiente para enfrentar los desafíos del *marketing* digital y el capitalismo de vigilancia[30], abogando por la adopción urgente de una Ley de Protección de Datos Personales, alineada con los estándares regionales e interamericanos.

El fallo fortaleció la Ley «No Molestar» al consolidar el derecho a la autodeterminación informativa y el derecho de exclusión frente a la publicidad no deseada, estableciendo que la oposición del usuario debe prevalecer sobre la libertad de empresa. Asimismo, validó el Registro Nacional «No Molestar» como un mecanismo legítimo de exclusión (modelo *opt-out*), cuyo desconocimiento constituye un tratamiento ilegítimo de datos personales, y reforzó el rol de SEDECO como autoridad competente para fiscalizar y sancionar infracciones en materia de publicidad no autorizada.

Más allá de la sanción específica, el caso puso en evidencia las carencias del marco legal paraguayo ante las nuevas dinámicas del *marketing* digital. Resaltó la necesidad de una Ley general de Protección de Datos Personales, dado que el marco actual es insuficiente, pese al reconocimiento constitucional del derecho a la privacidad. También expuso las tensiones entre las prácticas comerciales basadas en la explotación de datos y el principio de consentimiento libre, expreso e informado, especialmente en los contratos de adhesión del sector de telecomunicaciones. Además,

27 Corte Suprema de Justicia de la República del Paraguay, «AMX Paraguay S.A. c/ Resolución N.º 983/2020 s/ acción de inconstitucionalidad», Sentencia N.º 495/2024.
«Solicitud #93826. Pregunta sobre sentencia 495/2024 - Caso SEDECO c/ AMX», *Portal Unificado de Información Pública*, acceso el 20 de octubre de 2025, https://bit.ly/4i4Fmvl

28 Antonia Bogado, *El caso Claro, SEDECO y la Ley «No Molestar»: Un hito judicial, derechos digitales y publicidad invasiva en Paraguay* (Asunción: TEDIC, 2025), https://bit.ly/40DMG3p

29 Ley N.º 5830/17, *SILPy - Sistema de Información Legislativa*, acceso el 20 de octubre de 2025, https://bit.ly/47WDr7d

30 El capitalismo de vigilancia se refiere a un modelo económico en el que las empresas recopilan, procesan y comercializan datos personales a gran escala para predecir y modificar comportamientos, generando beneficios comerciales y ejerciendo un control significativo sobre los usuarios. Véase Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

aunque SEDECO interpreta que la Ley N.º 5830/17 podría aplicarse a canales como WhatsApp, el caso demuestra que la normativa carece de mecanismos eficaces para enfrentar el tratamiento de datos en entornos digitales.

Finalmente, el caso ha impulsado propuestas de mejora normativa promovidas por SEDECO y TEDIC, orientadas a fortalecer la protección de los consumidores y sus datos personales. Entre las principales se destacan: la responsabilidad solidaria del emisor de mensajes no deseados, la adopción de un modelo de inscripción automática (*opt-in*) en el Registro «No Molestar», la implementación de estándares claros de consentimiento y la creación de un marco integral de derechos ARCO (acceso, rectificación, cancelación y oposición), aplicable a todos los canales de comunicación.

CONCLUSIONES

De cara al 2026, el panorama de los derechos digitales en Paraguay muestra luces y sombras. El avance más esperanzador es la sanción del proyecto de Ley de Protección de Datos Personales, marcando un hito tras años de ausencia de un marco integral de resguardo de la privacidad y la autodeterminación informativa. Sin embargo, el país continúa enfrentando una profunda vulnerabilidad normativa y operativa frente a las amenazas tecnológicas, el incremento de la violencia digital y el recrudecimiento de la vigilancia estatal.

En el ámbito del *marketing* digital, el fallo Claro vs. SEDECO reafirmó el derecho ciudadano a decidir sobre el uso de sus datos y la validez de la Ley «No Molestar», pero también evidenció la fragmentación regulatoria y la incapacidad del Estado para responder a las dinámicas del capitalismo de vigilancia. En paralelo, el uso de la inteligencia artificial carece de una estrategia nacional y de marcos éticos claros, generando riesgos vinculados con la soberanía tecnológica, los sesgos algorítmicos, el desempleo tecnológico, la desinformación y la expansión del reconocimiento facial sin controles adecuados.

El año 2025 estuvo marcado además por graves vulneraciones de derechos a raíz de la vigilancia digital ejercida por el Estado. El espionaje ilegal contra jóvenes de la «Generación Z» durante la organización de manifestaciones demostró una intromisión injustificada en espacios privados de comunicación, afectando la privacidad, la libertad de expresión y la libre asociación. En paralelo, la expansión de tecnologías biométricas, como el reconocimiento facial o los sistemas de pago y acceso implementados en la Expo Paraguay 2025, reveló riesgos de exclusión y concentración de datos sensibles en manos de actores privados, sin salvaguardas ni fiscalización ciudadana.

En materia de ciberseguridad, los ciberataques y las filtraciones que afectaron a diversas entidades estatales evidenciaron la fragilidad institucional del país y su dependencia tecnológica. Estas brechas no solo ponen en riesgo la información estratégica y la soberanía digital, sino que también pueden afectar la estabilidad democrática al comprometer derechos políticos y la confianza pública. Por ello, es crucial destacar que la ciberseguridad va más allá de la protección tecnológica, pues se entrelaza con la integridad institucional y los derechos fundamentales. La seguridad digital está vinculada tanto con la fortaleza de las instituciones democráticas como con la autonomía estatal en la toma de decisiones estratégicas. Incidentes como el ataque cibernético coordinado que afectó a más de diez entidades del Estado paraguayo, incluidas la Presidencia y la Cámara de Diputados, o los ciberataques dirigidos a sabotear infraestructuras críticas —como hidroeléctricas o máquinas de votación— ilustran cómo la vulnerabilidad digital puede repercutir en derechos políticos, como la participación, y en la estabilidad democrática, así como en otros derechos socioeconómicos.

Por último, aunque la aprobación de la Estrategia Nacional de Ciberseguridad 2025-2028 representa un avance institucional al consolidar al MITIC como autoridad nacional, el enfoque del documento sigue siendo predominantemente técnico y punitivo, con escasa articulación de derechos humanos y participación multisectorial. La ausencia de ministerios e instituciones sociales en su diseño, la falta de mecanismos de participación civil y el énfasis en la penalización por sobre la prevención refuerzan el riesgo de que la ciberseguridad se transforme en una herramienta de control más que en una política de protección.

Para culminar, es importante resaltar que el Paraguay transita un momento decisivo: la consolidación de un marco normativo moderno y garantista dependerá de que las políticas digitales se diseñen desde una perspectiva de derechos humanos, transparencia y participación social, asegurando que la tecnología sirva a la libertad y no al control.

RECOMENDACIONES

- → Promulgar inmediatamente la Ley general de Protección de Datos Personales y reglamentarla de forma urgente para poder ejercer este derecho.

- → Reformar la Ley «No molestar» mediante la inscripción automática de las personas usuarias (modelo *opt-in*), lo que garantizaría un consentimiento más robusto y respetuoso.

- Transformar su enfoque de ciberseguridad, pasando de un modelo predominantemente técnico y punitivo a uno centrado en las personas, la prevención y la protección de los derechos.
- Transparentar los mecanismos tecnológicos de vigilancia, como el uso de cámaras con reconocimiento facial, para evitar abusos.
- Garantizar que la Ley N.º 7177 de Identidad Digital se aplique conforme a los estándares de necesidad y proporcionalidad establecidos por la Corte Interamericana de Derechos Humanos.
- Crear marcos regulatorios para la IA basados en principios de transparencia, responsabilidad y respeto a los derechos humanos.
- Fortalecer la educación digital y el pensamiento crítico como herramientas esenciales para enfrentar fenómenos como la desinformación.

Jazmín Ruiz Díaz Figueredo
Licenciada en Ciencias de la Comunicación (UNA). Magíster en Industrias Culturales y Creativas (King's College London). PhD en Cultura, Medios e Industrias Creativas (King's College London). Como investigadora, trabaja en la intersección de los estudios culturales y de género. Actualmente, se enfoca en temas de tecnología y cultura digital. Es Coordinadora de Proyectos de Género y Tecnología en TEDIC y cuenta con más de 15 años de experiencia en medios y gestión cultural.
Contacto: jazrd@tedic.org