

The background of the entire page is a dark purple. Overlaid on this are stylized, high-contrast illustrations of various people in motion. Each person is enclosed within a thin, light blue rectangular border, resembling a digital selection or tracking box. The people depicted include a man in a black t-shirt and white pants, a woman in a black tank top and white pants, a man in a white t-shirt and black shorts, a man in a white shirt and black pants sitting in a wheelchair, a man in a white t-shirt and black pants looking down, a woman in a white t-shirt and black pants, a man in a black t-shirt and black shorts, a woman in a white t-shirt and black pants, a man in a white t-shirt and black pants with a backpack, and a woman in a white t-shirt and black pants. The overall theme is digital surveillance and threats in a diverse population.

En la mira 2: Un panorama de las amenazas digitales en América Latina

En la mira 2: Un panorama de las amenazas digitales en América Latina

Esta publicación fue realizada por Derechos Digitales, organización independiente sin fines de lucro, fundada en el año 2005, cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en los entornos digitales en América Latina.

Supervisión general: Rafael Bonifaz

Coordinación y revisión: Rafael Bonifaz y Jamila Venturini

Análisis y redacción: Ximena Cuzcano

Investigación: Ximena Cuzcano

Revisión de estilo: Gastón Wahnish

Diseño: Diego Lepián

El presente informe es el resultado del trabajo conjunto realizado en el marco del Observatorio Latinoamericano de Amenazas Digitales (OLAD), una alianza de organizaciones latinoamericanas que incluyen a Código Sur (regional), Colnodo (Colombia), Conexión Segura (Venezuela), Derechos Digitales (regional), Escola de Ativismo (Brasil), Fundación Acceso (regional), Fundación InternetBolivia.org (Bolivia), Fundación Karisma (Colombia), Instituto Nupef (Brasil), LaLibre.net Tecnologías Comunitarias (Ecuador), MariaLab (Brasil), Social TIC (México), Sursiendo (México) y Taller de Comunicación Mujer (Ecuador).

Agosto, 2026

Cómo citar esta publicación: Derechos Digitales. (2026). En la mira 2: un panorama de las amenazas digitales en América Latina.

<https://www.derechosdigitales.org/recursos/en-la-mira-2>



Esta obra está disponible bajo licencia Creative Commons Atribución 4.0 Internacional
<https://creativecommons.org/licenses/by/4.0/deed.es>

Índice

1 Introducción	4
2 Metodología	7
3 Contexto de seguridad digital en América Latina	10
3.1. Normativa	11
3.2. Censura	14
3.3. Filtraciones de datos	18
3.4. Desinformación en elecciones	22
3.5. Ataques dirigidos	24
4 Áreas temáticas	29
4.1. Violencia de género facilitada por las tecnologías	30
4.1.1. Navegando Libres	31
4.1.2. S.O.S. Digital	32
4.1.3. Otros casos	33
4.2. Explotación de datos biométricos	34
4.3. Cortes de internet	38
4.4. Vigilancia	41
5 Conclusiones	48



1. Introducción

1 Introducción

Internet y las tecnologías digitales son un espacio central para el ejercicio de derechos humanos en América Latina. A través de ellas, las comunidades acceden a información y servicios esenciales, activistas se organizan y coordinan, y periodistas documentan abusos de poder e informan. Mantener ese espacio libre y seguro es una condición necesaria para el ejercicio de derechos fundamentales. Sin embargo, ese mismo espacio se ha convertido también en escenario de vigilancia, censura, violencia y control. A diferencia de los reportes de ciberseguridad enfocados en impactos económicos y comerciales, este informe es un esfuerzo por visibilizar cómo las amenazas y ataques digitales afectan la labor de la sociedad civil y el ejercicio de derechos fundamentales en la región.

En la mira 2: un panorama de las amenazas digitales en América Latina es resultado del trabajo liderado por Derechos Digitales en el marco del Observatorio Latinoamericano de Amenazas Digitales (OLAD), una alianza de organizaciones latinoamericanas dedicadas a la defensa de los derechos humanos en el espacio digital. El Observatorio permite el intercambio de conocimientos y experiencias relacionadas con seguridad digital, y es una plataforma de monitoreo de incidentes desde una perspectiva de derechos humanos e interés público.

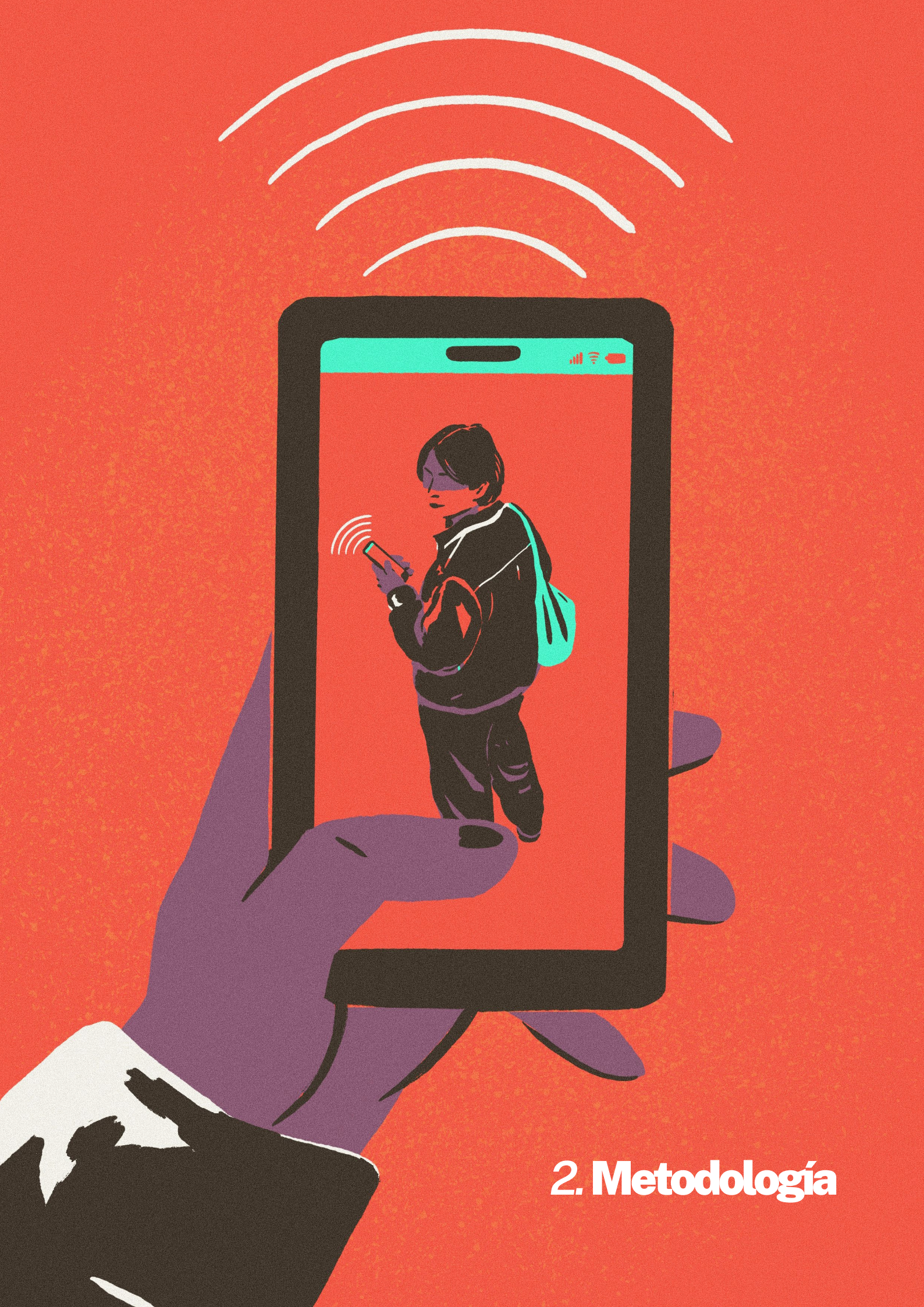
Forman parte de esta alianza las organizaciones: Código Sur (regional), Colnodo (Colombia), Conexión Segura (Venezuela), Derechos Digitales (regional), Escola de Ativismo (Brasil), Fundación Acceso (regional), Fundación InternetBolivia.org (Bolivia), Fundación Karisma (Colombia), Instituto Nupef (Brasil), LaLibre.net Tecnologías Comunitarias (Ecuador), MariaLab (Brasil), Social TIC (México),

Sursiendo (México) y Taller de Comunicación Mujer (Ecuador). Esta segunda entrega se apoyó de manera especial en los reportes e investigaciones producidos por varias de estas organizaciones.

Cada una de las organizaciones del OLAD cumple funciones distintas según el contexto de su país y su área de especialización. Desde distintos territorios y campos de acción, producen conocimiento, acompañan casos, investigan amenazas y alertan sobre prácticas que afectan los derechos en línea. Derechos Digitales, a partir del trabajo de las organizaciones y a través de un monitoreo periódico, ha liderado la redacción del presente reporte con el fin de visibilizar cómo las amenazas digitales afectan el ejercicio de derechos en América Latina.

En la mira 2 da continuidad al trabajo del primer informe de esta serie. Entendemos que la documentación acumulada a lo largo del tiempo es en sí misma una herramienta de incidencia y memoria. También constituye un mecanismo esencial para la futura rendición de cuentas pues, en contextos autoritarios donde hoy no existen condiciones para investigar, sancionar o reparar las violaciones, preservar evidencia y mantener registros rigurosos permite sostener la verdad de los hechos, fortalecer los procesos de justicia —para cuando las condiciones cambien— e incluso reducir el riesgo de que estas agresiones queden en la impunidad.

El informe se organiza en dos grandes bloques. El primero, *Contexto de seguridad digital en América Latina*, ofrece un panorama regional a través de cinco ejes: los desarrollos normativos del período, la censura en entornos digitales, las filtraciones de datos, la desinformación en procesos electorales y los ataques dirigidos. El segundo bloque, *Áreas temáticas*, profundiza en cuatro tendencias de incidentes digitales durante este período: la vigilancia, la explotación de datos biométricos, los apagones de internet y la violencia de género facilitada por las tecnologías.



2. Metodología

2 Metodología

El informe *En la mira 2* presenta un panorama regional de incidentes de seguridad digital que afectan el ejercicio de derechos humanos en América Latina. El período de análisis comprende junio de 2024 a mayo de 2025. Para efectos de este informe, se consideran incidentes aquellos eventos vinculados al uso, control o abuso de tecnologías digitales que generan impactos sobre derechos como la libertad de expresión, privacidad y protección de datos, el acceso a la información, la integridad y seguridad de personas y colectivos, así como la participación cívica en entornos digitales.

La información analizada fue recolectada a través de dos vías complementarias. En primer lugar, se realizó un monitoreo sistemático semanal de fuentes abiertas, principalmente noticias publicadas en medios de comunicación, reportes disponibles en internet y seguimiento a incidentes de filtración de datos disponibles en línea. Este enfoque permite identificar tendencias regionales y documentar incidentes con visibilidad pública; sin embargo, presenta limitaciones relevantes. La cobertura mediática es desigual entre países, muchos incidentes no llegan a publicarse y, en contextos de censura o debilidad de la prensa, una parte significativa de los hechos queda fuera del registro público.

En segundo lugar, el reporte incorpora información y análisis provenientes de las organizaciones que integran el OLAD, las cuales trabajan directamente en el acompañamiento a personas y organizaciones afectadas por ataques digitales, investigación y/o monitoreo de este tipo de incidentes en la región. Esta articulación permite complementar los vacíos del monitoreo de noticias y comprender dinámicas que no siempre son visibles en fuentes abiertas. No obstante, esta vía también enfrenta limitaciones, ya que no todos los casos pueden ser difundidos públicamente sin aumentar riesgos para las personas afectadas o

para quienes acompañan los procesos. En consecuencia, los hallazgos del informe no deben interpretarse como un ranking de incidentes ni como una medición comparativa entre países, sino como un análisis situado de patrones y dinámicas regionales.

Durante el período analizado, estas limitaciones se han visto agravadas por un entorno global cada vez más adverso para la sociedad civil. Diversas organizaciones enfrentan restricciones al espacio cívico, mayores niveles de vigilancia y estigmatización de su labor, así como dificultades de sostenibilidad financiera, en un contexto de reducción o congelamiento de fondos internacionales destinados al trabajo en derechos humanos y tecnología. Estas condiciones impactan directamente la capacidad de monitoreo y documentación continua de casos, y deben ser consideradas al interpretar los hallazgos del reporte.

Finalmente, la información recolectada fue organizada en líneas temáticas que permiten analizar patrones y tipos de incidentes a nivel regional. En todos los casos, se aplicó un criterio de verificación razonable, priorizando la trazabilidad de las fuentes y evitando conclusiones que no pudieran sostenerse con la evidencia disponible públicamente. Asimismo, el informe adopta un enfoque de no daño, cuidando la publicación de detalles que pudieran facilitar revictimización o riesgos adicionales para personas y comunidades afectadas.



3. Contexto de seguridad digital en América Latina

3 Contexto de seguridad digital en América Latina

Este capítulo ofrece un panorama del contexto de seguridad digital en América Latina durante el período analizado, a partir de un proceso de sistematización y análisis del monitoreo de fuentes abiertas. Más que presentar un inventario exhaustivo de incidentes, busca situar los principales fenómenos observados en la región y comprender cómo se manifiestan de manera transversal, diferenciando los impactos en distintos países y grupos sociales.

3.1. Normativa

Durante el monitoreo regional se identificaron desarrollos normativos relevantes en distintos países de América Latina que inciden de manera directa en el ejercicio de derechos humanos en el entorno digital. En este marco, emergen de forma recurrente iniciativas legislativas y regulatorias vinculadas a la vigilancia estatal, la limitación de la libertad de expresión —incluyendo mecanismos de censura— y restricciones al acceso a la información pública, entre otros. Estos ejes reflejan respuestas estatales que configuran el contexto político y legal que hace posible —y en algunos casos legítima— los incidentes de seguridad digital analizados en las secciones siguientes.

Cabe señalar que los desarrollos normativos descritos corresponden al estado de cada proceso legislativo o regulatorio al cierre del período analizado. Dado el carácter dinámico de estos procesos, algunas iniciativas pueden haber avanzado, sido modificadas o archivadas con posterioridad a esa fecha, por lo que su evolución seguirá siendo parte del monitoreo continuo que da origen a este informe.

Una primera tendencia normativa observable es la expansión de marcos normativos que amplían las **facultades estatales de vigilancia** en entornos digitales, generalmente justificadas bajo discursos de seguridad nacional y orden público. En **Argentina**, la Resolución 428/2024 del Ministerio de Seguridad formalizó un protocolo para la prevención del delito que habilita el monitoreo sistemático de fuentes abiertas y el uso de tecnologías automatizadas para análisis de información en línea¹. Al cierre de este reporte, el Decreto 383/2025 incorporó el ciberpatrullaje como facultad explícita de esta fuerza, sin necesidad de autorización judicial cuando se trate de fuentes abiertas^{2,3}. En **Paraguay**, la Ley 7269/2024 incorporó la vigilancia biométrica obligatoria mediante sistemas de reconocimiento facial en estadios de fútbol, extendiendo prácticas de monitoreo masivo a espacios públicos⁴. En **México**, diversas iniciativas de reforma a la Ley de Seguridad Nacional ampliaron de forma ambigua la noción de amenazas a la seguridad, abriendo la puerta a una expansión de las facultades de vigilancia estatal y de control de la información⁵. En **Ecuador**, la aprobación de una nueva Ley de Inteligencia creó un Sistema Nacional de Inteligencia con amplias atribuciones para interceptar comunicaciones y acceder a datos de telecomunicaciones sin orden judicial⁶. Al cierre de este reporte, la ley se encuentra bajo análisis de la Corte Constitucional, tras la presentación de acciones de inconstitucionalidad que cuestionan la compatibilidad de estas facultades con derechos fundamentales; no obstante, el Ejecutivo ya emitió el reglamento de aplicación, que faculta a las entidades de inteligencia a requerir directamente a las operadoras de telecomunicaciones información sobre geolocalización, tráfico de datos y registros de llamadas, sin orden judicial⁷. En **Venezuela**, la creación por decreto del Consejo Nacional de Ciberseguridad consolidó un enfoque de cibervigilancia estatal con facultades extensas, bajo una narrativa de amenazas cibernéticas asociadas a redes sociales y actores opositores⁸.

En sentido contrario, en **Colombia** se radicó el Proyecto de Ley Estatutaria 225, que buscaba reformar la Ley 1621 de 2013 para reforzar la protección a los derechos humanos y fortalecer el marco jurídico de los organismos que llevan a cabo actividades de inteligencia y contrainteligencia, en cumplimiento de una sentencia

1. Juan Manuel García, “¡Cuidado, te están vigilando!”, Derechos Digitales (Junio 14, 2024). Disponible en: <https://www.derechosdigitales.org/recursos/cuidado-te-estan-vigilando/>

2. República Argentina, “Decreto 383/2025”, Boletín Oficial de la República Argentina (Junio 16, 2025). Disponible en: <https://www.boletinoficial.gob.ar/detalleAviso/primera/326993/20250617>

3. Rosario Marina, “Ciberpatrullaje: qué dice el nuevo decreto y qué implican los cambios en la Policía Federal”, Chequeado (Junio 18, 2025). Disponible en: <https://chequeado.com/el-explicador/ciberpatrullaje-que-dice-el-nuevo-decreto-y-que-implican-los-cambios-en-la-policia-federal/>

4. Mariela Cuevas, “Retos y deudas para la seguridad y protección en el entorno digital”, Derechos Humanos Paraguay 2024 (Diciembre 12, 2024). Disponible en: <https://ddhh2024.codehupy.org.py/retos-y-deudas-para-la-seguridad-y-proteccion-en-el-entorno-digital/>

5. R3D, “Iniciativas para ampliar el catálogo de amenazas a la seguridad nacional ponen en riesgo los derechos humanos en el entorno digital”, R3D: Red en Defensa de los Derechos Digitales (Octubre 14, 2024). Disponible en: <https://r3d.mx/2024/10/14/iniciativas-para-ampliar-el-catalogo-de-amenazas-a-la-seguridad-nacional-ponen-en-riesgo-los-derechos-humanos-en-el-entorno-digital/>

6. Carolina Mella, “Noboa abre la puerta al espionaje masivo en Ecuador con una nueva ley de inteligencia”, El País América (Junio 23, 2025). Disponible en: <https://elpais.com/america/2025-06-23/noboa-abre-la-puerta-al-espionaje-masivo-en-ecuador-con-una-nueva-ley-de-inteligencia.html>

7. Redacción Primicias, “Listo el reglamento para Ley de Inteligencia, que obligará a las telefónicas a entregar información”, Primicias (Julio 14, 2025). Disponible en: <https://www.primicias.ec/politica/reglamento-ley-inteligencia-ecuador-telefonicas-daniel-noboa-documento-texto-descarga-100652/>

8. El Estímulo, “Consejo Nacional de Ciberseguridad: de qué se trata el nuevo organismo creado por Maduro”, El Estímulo (Agosto 21, 2024). Disponible en: <https://elestimulo.com/venezuela/2024-08-21/consejo-nacional-de-ciberseguridad/>

de la Corte Interamericana de Derechos Humanos⁹. El proyecto recibió ponencia positiva para primer debate en noviembre de 2024, pero no fue debatido antes de finalizar la legislatura, por lo que habría sido archivado¹⁰.

Otra línea normativa relevante incide directamente sobre **la libertad de expresión y la implementación de mecanismos de censura digital**. En **El Salvador**, la aprobación de la Ley de Ciberseguridad y la creación de la Agencia de Ciberseguridad del Estado (ACE) consolidaron un esquema institucional altamente centralizado con facultades de regulación, supervisión y sanción que podrían facilitar la eliminación de contenidos en línea¹¹. En **Colombia**, el Proyecto de Ley 023 de 2023, debatido durante 2024, propone la creación de una Agencia de Seguridad Digital con facultades excepcionales para ordenar el cese de operaciones en el ciberespacio que consiste en la interrupción temporal de las plataformas, o servicios digitales en contextos definidos como de crisis, cuya aplicación podría implicar la suspensión de redes sociales o medios digitales y con ello, afectar la circulación de información¹². En **Cuba**, la Ley de Comunicación Social, vigente desde 2024, establece un régimen integral de regulación de contenidos y medios digitales que refuerza el control estatal sobre la producción y circulación de información, afectando de manera particular a medios independientes y expresiones no estatales¹³. En **Nicaragua**, la reforma a la Ley 1042, Ley Especial de Ciberdelitos, amplió la tipificación de conductas vinculadas a la difusión de información en línea y configura un marco que se ha utilizado para sancionar expresiones digitales y generar un efecto inhibitorio sobre el periodismo, activismo y sociedad civil¹⁴.

De manera similar, se observan reformas legales que debilitan los mecanismos institucionales de **acceso a la información pública**, lo que afecta la transparencia y rendición de cuentas. En **México**, las reformas constitucionales aprobadas entre 2024 y 2025 eliminaron al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como órgano autónomo¹⁵. De esta manera se limita la capacidad ciudadana para conocer y supervisar las actuaciones del Estado y participar de manera informada en asuntos públicos. En , las modificaciones introducidas en 2024 al régimen de acceso a la información pública ampliaron las causales de reserva y restringieron el alcance de lo considerado

9. Clara López Obregón, "INFORME DE PONENCIA AL PROYECTO DE LEY ESTATUTARIA NO. 225 DE 2024 SENADO", Comisión Primera Constitucional Permanente del Senado de la República de Colombia (Octubre 1, 2024). Disponible en: <https://www.comisionprimeras Senado.com/documentos-pendientes-de-publicacion/ponencias-y-textos-aprobados/4148-ponencia-ple-225-de-2024-inteligencia-y-contrainteligencia/file>

10. Conforme al artículo 153 de la Constitución Política de Colombia, las leyes estatutarias deben tramitarse y aprobarse dentro de una sola legislatura.

11. Human Rights Watch, "El Salvador: Nuevas leyes amenazan la libertad de expresión y la privacidad", Human Rights Watch (Diciembre 12, 2024). Disponible en: <https://www.hrw.org/es/news/2024/12/12/el-salvador-nuevas-leyes-amenazan-la-libertad-de-expresion-y-la-privacidad>

12. Mateo García Agudelo, "¿Gobierno del presidente Petro busca, con proyecto de ley, facultades para apagar las redes sociales en Colombia?", El Tiempo (Septiembre 25, 2024). Disponible en: <https://www.eltiempo.com/politica/congreso/gobierno-del-presidente-petro-busca-con-proyecto-de-ley-facultades-para-apagar-las-redes-sociales-en-colombia-3384505>

13. Infobae, "Persecución en Cuba: el régimen publicó la controvertida Ley de Comunicación Social", Infobae (Junio 6, 2024). Disponible en: <https://www.infobae.com/america/america-latina/2024/06/06/persecucion-en-cuba-el-regimen-publico-la-controvertida-ley-de-comunicacion-social/>

14. Infobae, "Denuncian que la ley de ciberdelitos en Nicaragua es 'devastadora' para los periodistas", Infobae (Octubre 8, 2024). Disponible en: <https://www.infobae.com/america/america-latina/2024/10/08/denuncian-que-la-ley-de-ciberdelitos-en-nicaragua-es-devastadora-para-los-periodistas/>

15. R3D, "Réquiem por el INAI: un retroceso para la defensa de los derechos digitales", R3D: Red en Defensa de los Derechos Digitales (Diciembre 11, 2024). Disponible en: <https://r3d.mx/2024/12/11/requiem-por-el-inai-un-retroceso-para-la-defensa-de-los-derechos-digitales/>

información pública¹⁶. Esta reforma reduce la obligación estatal de divulgar información de interés público y debilita la capacidad de control ciudadano.

En paralelo, persisten tensiones normativas en materia de **protección de datos personales**, donde avances normativos coexisten con marcos legales que habilitan prácticas de vigilancia. En **Chile**, la aprobación de la Ley 21.719 de Protección de Datos Personales y de la Ley 21.663, Ley Marco de Ciberseguridad, fortaleció la institucionalidad en la materia y amplió derechos¹⁷. Sin embargo, estos avances conviven con normas que autorizan el uso de tecnologías de vigilancia, como los dispositivos de interceptación de comunicaciones (IMSI catchers), en el marco de la legislación antiterrorista¹⁸. En **El Salvador**, se implementó la Ley de Protección de Datos Personales en paralelo a un marco de ciberseguridad, en el que los objetivos de seguridad nacional y orden público se definen de forma amplia e imprecisa y con salvaguardas institucionales limitadas¹⁹. Esto genera dudas sobre la primacía real de los derechos de las personas frente a objetivos de seguridad.

3.2. Censura

El panorama de la censura en entornos digitales en América Latina entre junio 2024 y mayo 2025 revela un ecosistema de control cada vez más adaptable y técnicamente complejo. Los Estados han combinado distintas técnicas de bloqueo de infraestructura con la presión sobre agentes privados, y la persecución legal para crear un efecto asfixiante a la libertad de expresión en línea. Estas medidas no son aisladas, sino que tienden a intensificarse de manera estratégica durante coyunturas críticas como procesos electorales o protestas sociales, y a combinar recursos técnicos con mecanismos institucionales o coercitivos. Además, impactan con mayor severidad en periodistas, activistas y personas con menos recursos técnicos para eludir bloqueos, profundizando las brechas digitales y de acceso a la información.

A continuación, se describen los principales incidentes observados en ese sentido, organizados por país.

16. Fernanda González, “Javier Milei decreta nuevos límites al acceso a la información pública en Argentina”, WIRED (Septiembre 3, 2024). Disponible en: <https://es.wired.com/articulos/milei-decreta-nuevos-limites-al-acceso-a-la-informacion-publica-en-argentina>

17. Juan Carlos Lara, “Los desafíos de la nueva Ley de Protección de Datos Personales”, CIPER Chile (Enero 28, 2025). Disponible en: <https://www.ciperchile.cl/2025/01/28/los-desafios-de-la-nueva-ley-de-proteccion-de-datos-personales/>

18. Helen Mora, “En medio de polémica por lmsi catcher: Congreso aprueba ley antiterrorista y despacha proyecto al Ejecutivo”, La Tercera (Diciembre 11, 2024). Disponible en: <https://www.latercera.com/politica/noticia/en-medio-de-ten-sa-sesion-congreso-aprueba-ley-antiterrorista/BY2SGOUJONH5JHEGFBSLC5LZR4/>

19. Human Rights Watch, “El Salvador: Nuevas leyes amenazan la libertad de expresión y la privacidad”, Human Rights Watch (Diciembre 12, 2024). Disponible en: <https://www.hrw.org/es/news/2024/12/12/el-salvador-nuevas-leyes-amenazan-la-libertad-de-expresion-y-la-privacidad>

Con relación al **bloqueo de plataformas y redes sociales**, tras las elecciones de 2024, el gobierno de **Venezuela**, a través de órdenes impartidas por la Comisión Nacional de Telecomunicaciones (CONATEL) a los proveedores de internet, ejecutó una ola masiva de bloqueos que afectó a plataformas como Signal, X, TikTok, Telegram y YouTube^{20 21 22 23}. Incluso se bloquearon servicios corporativos como Microsoft Teams, sitios de estadísticas como Statista y plataformas de entretenimiento como Disney+, Max y Amazon Prime Video²⁴. La censura alcanzó una escala particularmente crítica según el informe de VE Sin Filtro²⁵, entre julio de 2024 y enero de 2025 se documentaron 79 nuevos bloqueos a sitios web, sumándose a 89 preexistentes, muchos de ellos contra medios independientes. A ellos se sumó el bloqueo de sitios web de proveedores de VPN²⁶ como Proton y Windscribe, con el objetivo de impedir que la ciudadanía eludiera las restricciones impuestas y proteja su privacidad en línea.

Además, la operadora de internet (ISP por sus siglas en inglés) estatal CANTV bloqueó más de 30 servidores DNS públicos, incluyendo los de Google y Cloudflare²⁷. El DNS funciona como una “guía telefónica” de internet: convierte nombres de dominio (por ejemplo, la dirección de un sitio web) en números IP que permiten acceder al contenido. En la práctica, la mayoría de personas utiliza el DNS que provee su operador de internet, como CANTV. Ese control le permite al proveedor restringir el acceso a determinados sitios al impedir o manipular la resolución DNS. En estos escenarios, una alternativa común es cambiar el proveedor de DNS para intentar recuperar el acceso.

Asimismo, se observaron formas de censura orientadas a afectar la disponibilidad de medios. En agosto de 2024, el sitio del diario TalCual sufrió un ataque de denegación de servicio distribuido (DDoS por sus siglas en inglés), una técnica que consiste en saturar un servidor con tráfico masivo desde varios lugares para hacerlo inaccesible, que afectó el acceso durante aproximadamente cuatro horas²⁸.

En **Brasil**, el Supremo Tribunal Federal ordenó la suspensión total de X como resultado del desacato reiterado de la plataforma a órdenes judiciales de designar

20. Regina García Cano, “Maduro suspends X social network in Venezuela for 10 days”, AP News (Agosto 9, 2024). Disponible en: <https://apnews.com/article/venezuela-elections-suspension-x-elon-musk-59bb734bdd0c8cc4082d6a0cb0f5af25>

21. Sergio Henostroza, “Usuarios reportan bloqueo masivo de TikTok en Venezuela y responsabilizan al régimen de Nicolás Maduro”, La República (Septiembre 29, 2024). Disponible en: <https://larepublica.pe/mundo/venezuela/2024/09/28/usuarios-reportan-bloqueo-masivo-de-tiktok-en-venezuela-y-responsabilizan-al-regimen-de-nicolas-maduro-lrtmc-613984>

22. Jay Peters, “Signal Has Been Blocked by Venezuela and Russia”, The Verge (Agosto 9, 2024). Disponible en: <https://www.theverge.com/2024/8/9/24217008/signal-blocked-venezuela-russia>

23. VE sin Filtro, “Bloquean nuevamente Telegram en Venezuela”, [@vesinfiltro] (Mayo 2, 2025). Disponible en: <https://x.com/vesinfiltro/status/1918276217746174061>

24. En la práctica, estos bloqueos suelen implementarse mediante interferencias técnicas, frecuentemente a nivel de DNS (en la resolución de nombres de dominio), para impedir el acceso sin cortar toda la conexión a internet.

25. VE sin Filtro, “Redes de control: Censura y represión digital en las elecciones presidenciales en Venezuela”, VE sin Filtro (2024). Disponible en: https://vesinfiltro.org/res/files/informe-presidenciales_2024-VEsinFiltro.pdf

26. Una Red Privada Virtual (VPN, por sus siglas en inglés) es una herramienta que cifra la conexión a internet y redirige el tráfico a través de servidores en otros países, permitiendo navegar de forma privada y eludir bloqueos geográficos o restricciones impuestas por proveedores de internet.

27. Redacción Voz de América, “Venezuela muestra ‘cifras alarmantes’ de censura digital, denuncia Ve Sin Filtro”, Voz de América (Marzo 14, 2025). Disponible en: <https://www.vozdeamerica.com/a/venezuela-cifras-alarmantes-censura-digital/8010029.html>

28. IPYS Venezuela, “Sitio web del diario TalCual fue objeto de un ataque DDoS”, Voces del Sur (Agosto 12, 2024). Disponible en: <https://vocesdelsur.unidas.org/incidentes/sitio-web-del-diario-talcual-fue-objeto-de-un-ataque-ddos/>

un representante legal en el país y eliminar cuentas vinculadas a la desinformación. La decisión también estableció sanciones a quienes intentaran evadir la suspensión mediante VPN. Si bien la suspensión tiene base legal en el Marco Civil de Internet, su alcance generalizado afectó a la totalidad de personas usuarias de la plataforma en el país, planteando interrogantes sobre su proporcionalidad frente a los estándares interamericanos en materia de libertad de expresión²⁹.

En **Colombia**, la entidad estatal Coljuegos —encargada de regular juegos de suerte y azar— ordenó a los proveedores de internet el bloqueo de Reddit, al considerar que el dominio estaba vinculado a operadores de apuestas no autorizados, bajo las facultades de la Ley 1753 de 2015³⁰. El bloqueo se ejecutó mediante redireccionamientos y restricciones por DNS, medida que fue confirmada a través de pruebas independientes realizadas con la herramienta OONI³¹. Aunque la medida fue temporal, generó dudas sobre su proporcionalidad y la falta de claridad en los criterios con que se incluyen sitios web en las listas oficiales de bloqueo³².

Con relación a los **ataques e intervenciones en la infraestructura de internet y los sistemas de nombres de dominio (DNS)**, en **Nicaragua**, la Universidad Nacional de Ingeniería (UNI), institución estatal administradora del dominio nacional .ni, a través de NIC.NI, bloqueó arbitrariamente, sin que mediara orden documentada ni notificación, los dominios de medios independientes como Confidencial, La Prensa, Onda Local y 100% Noticias, forzándolos a migrar a dominios internacionales para continuar operando³³.

Un intento similar ocurrió en **República Dominicana**, cuando la empresa estadounidense Network Solutions emitió un ultimátum al diario Listín Diario, exigiéndole borrar un reportaje sobre corrupción, bajo amenaza de suspender su alojamiento web³⁴. La empresa alegó una supuesta infracción de sus términos de servicio tras recibir una solicitud de remoción³⁵. Con este caso se evidencia el rol que las empresas privadas operando en niveles de infraestructura pueden tener en la imposición de mecanismos indirectos de censura, al utilizar cláusulas contractuales vagas para silenciar información de interés público.

29. Lucía Camacho, “La suspensión de X en Brasil, y la vigencia del Estado de Derecho”, Derechos Digitales (Septiembre 11, 2024). Disponible en: <https://www.derechosdigitales.org/recursos/la-suspension-de-x-en-brasil-y-la-vigencia-del-estado-de-derecho/>

30. Fundación Karisma, “Las dudas que quedan tras el bloqueo de Reddit en Colombia”, Fundación Karisma (Junio 7, 2024). Disponible en: <https://blog.karisma.org.co/las-dudas-que-quedan-tras-el-bloqueo-de-reddit-en-colombia/>

31. OONI es un proyecto y conjunto de herramientas de software libre desarrollado por The Tor Project, cuyo objetivo es monitorear, medir y documentar la censura en internet, la manipulación del tráfico y la interferencia en las redes de telecomunicaciones a nivel global. Disponible en: <https://ooni.org/es/>

32. Lucía Camacho, “La suspensión de X en Brasil, y la vigencia del Estado de Derecho”, Derechos Digitales (Septiembre 11, 2024). Disponible en: <https://www.derechosdigitales.org/recursos/la-suspension-de-x-en-brasil-y-la-vigencia-del-estado-de-derecho/>

33. Redacción Confidencial, “UNI bloquea los dominios .ni de cinco medios de comunicación en Nicaragua”, Confidencial (Marzo 14, 2025). Disponible en: <https://confidencial.digital/nacion/bloquean-dominios-ni-de-medios-de-comunicacion-en-nicaragua/>

34. SWI swissinfo.ch, “La SIP denuncia intento de censura contra el medio Listín Diario en República Dominicana”, SWI swissinfo.ch (Mayo 15, 2025). Disponible en: <https://www.swissinfo.ch/spa/la-sip-denuncia-intento-de-censura-contra-el-medio-listin-diario-en-republica-dominicana/89328856>

35. Miguel Franjul, “COMUNICADO DEL LISTÍN DIARIO ANTE CENSURA DIGITAL”, Listín Diario (Mayo 15, 2025). Disponible en: https://listindiario.com/la-republica/20250515/comunicado-listin-diario-censura-digital_857815.html

En **Cuba**, el Estado utiliza la tecnología Deep Packet Inspection (DPI)³⁶ para analizar el tráfico en tiempo real y bloquear aplicaciones de mensajería cifrada como Signal y DeltaChat³⁷. A esta técnica se suman apagones completos de internet de liberados por parte de la estatal ETECSA durante movilizaciones sociales, además de aumentar las tarifas para limitar el acceso de la población³⁸.

También en **Cuba**, en agosto de 2024, una persona fue sentenciada a un año y medio de cárcel tras publicar un meme con imágenes de figuras del gobierno, y al menos otras cuatro fueron detenidas e interrogadas por publicaciones en redes³⁹. Entre septiembre y octubre, la oleada represiva provocó el cierre de al menos un medio, la citación a interrogatorio y amenaza de prisión a cuatro directores de medios, y la renuncia de al menos nueve periodistas y activistas^{40 41}.

Casos de persecución judicial se observaron en **Honduras**, donde el medio Honduriano fue investigado por “injuria con publicidad” tras informar, a través de una publicación en X, sobre tensiones internas en las Fuerzas Armadas⁴². En **El Salvador**, la Fiscalía preparó órdenes de captura contra periodistas de El Faro tras una investigación publicada en YouTube sobre pactos gubernamentales con pandillas⁴³.

36. El Deep Packet Inspection (DPI) es una tecnología de análisis de tráfico de red que, a diferencia de los métodos de filtrado convencionales, permite examinar el contenido completo de los paquetes de datos que circulan por internet, y no solo su origen o destino. Esto le permite a quien controla la red identificar y bloquear aplicaciones, protocolos o contenidos específicos de forma selectiva, incluso cuando se utilizan herramientas de cifrado.

37. Diktyon, “Informe #6 sobre la salud del Internet en Cuba”, Guardianes Digitales (Octubre, 2024). Disponible en: <https://guardianesdigitales.blogspot.com/2024/10/informe-6-sobre-la-salud-del-internet.html>

38. Infobae, “Crisis en Cuba: el régimen refuerza el control estatal sobre Internet y crece la censura en la isla”, Infobae (Junio 1, 2025). Disponible en: <https://www.infobae.com/america/america-latina/2025/06/01/crisis-en-cuba-el-regimen-refuerza-el-control-estatal-sobre-internet-y-crece-la-censura-en-la-isla/>

39. Yucabyte, “Violaciones de derechos digitales en Cuba (agosto de 2024)”, Yucabyte (Septiembre, 2024). Disponible en: <https://www.yucabyte.org/2024/09/26/violaciones-de-derechos-digitales-en-cuba-agosto-de-2024/>

40. Yucabyte, “Violaciones de derechos digitales en Cuba (septiembre de 2024)”, Yucabyte (Octubre 28, 2024). Disponible en: <https://www.yucabyte.org/2024/10/28/derechos-digitales-cuba-septiembre-2024/>

41. Yucabyte, “Violaciones de derechos digitales en Cuba (octubre de 2024)”, Yucabyte (Noviembre 27, 2024). Disponible en: <https://www.yucabyte.org/2024/11/27/violaciones-de-derechos-digitales-en-cuba-octubre-de-2024/>

42. ARTICLE 19, “Unidad Contra Delitos Informáticos de la Interpol de Honduras investiga a medio «Honduriano» por supuesto delito de injuria”, ARTICLE 19 (Febrero 2, 2025). Disponible en: <https://articulo19.org/unidad-contra-delitos-informaticos-de-la-interpol-de-honduras-investiga-a-medio-honduriano-por-supuesto-delito-de-injuria/>

43. FIDH, “El Salvador: escalada de persecución y ataques a la libertad de prensa contra el periódico digital El Faro”, Federación Internacional por los Derechos Humanos (Mayo 9, 2025). Disponible en: <https://www.fidh.org/es/region/americas/el-salvador/el-salvador-escalada-de-persecucion-y-ataques-a-la-libertad-de-prensa>

3.3. Filtraciones de datos

Estados y empresas almacenan grandes volúmenes de datos personales para operar servicios, administrar programas y gestionar trámites cotidianos. Cuando el tratamiento de datos se realiza sin estándares adecuados de seguridad y gobernanza o con procesos de tercerización poco controlados, aumenta la probabilidad de exposición o acceso indebido. En este contexto, las filtraciones de datos personales se consolidaron como uno de los fenómenos más recurrentes del escenario de seguridad digital en la región.

Una filtración ocurre cuando información personal o confidencial, almacenada por entidades públicas o privadas, es accedida por personas no autorizadas. Esto habilita su uso para fraude, extorsión, vigilancia o violencia. A diferencia de otros tipos de incidentes asociados a coyunturas específicas, las filtraciones responden a prácticas organizacionales deficientes que se repiten en distintos países y sectores, como la recolección excesiva de datos, la tercerización tecnológica sin controles adecuados, y la debilidad de mecanismos de protección y supervisión de accesos, en un contexto donde varios países de la región aún carecen de marcos regulatorios de protección de datos personales. En este reporte se identificaron casos específicos en 12 países⁴⁴, además de filtraciones de alcance regional.

Una de las formas más recurrentes de filtración identificadas no respondió a ciberataques sofisticados, sino a errores básicos de protección de la información. En particular, múltiples incidentes se originaron en **malas configuraciones**, donde bases de datos quedaron accesibles sin autenticación. En términos simples, esto equivale a dejar archivos confidenciales en un espacio público sin ningún tipo de cerradura. En **Colombia**, la aplicación de pagos GoPass dejó un contenedor de Google Cloud Storage⁴⁵ abierto, exponiendo datos de casi un millón de personas, incluyendo matrículas vehiculares y números de identificación tributaria⁴⁶.

En **Costa Rica**, una mala configuración en la infraestructura de Movistar dejó accesibles cerca de 650 mil archivos con documentos de identidad, permisos de trabajo y selfies utilizados en procesos de verificación de identidad⁴⁷. **A nivel regional**, la plataforma de banca digital Bankingly expuso datos personales y financieros de más de 135 mil clientes de cooperativas y entidades microfinancieras en países como Bolivia, Costa Rica, Ecuador, El Salvador, México y República Dominicana tras

44. Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, Honduras, México, Paraguay, Perú, Uruguay y Venezuela.

45. Google Cloud Storage: servicio de almacenamiento en la nube de Google que permite guardar y acceder a grandes volúmenes de datos mediante contenedores llamados buckets. Una configuración incorrecta de permisos puede hacer que estos buckets queden públicos y expongan información sensible sin autenticación.

46. Paulina Okunyté, "Cashless Toll Payments End with Massive Data Leak", Cybernews (Septiembre 19, 2024). Disponible en: <https://cybernews.com/security/gopass-colombia-data-leak/>

47. Alberto Payo, "Una brecha en Movistar Costa Rica deja accesibles cientos de miles de documentos de identidad", EscudoDigital (Febrero 27, 2025). Disponible en: https://www.escudodigital.com/ciberseguridad/brecha-en-movistar-costa-rica-deja-accesibles-cientos-miles-documentos-identidad_62456_102.html

utilizar contenedores de Azure⁴⁸ sin las medidas de seguridad adecuadas⁴⁹.

Otro conjunto relevante de incidentes estuvo asociado a la **vulnerabilidad de la cadena de suministro digital**, donde la filtración no se produce directamente en la organización principal, sino en proveedores tecnológicos que tienen acceso a sus sistemas. En **Perú**, la filtración de datos de clientes de Interbank se originó por el uso indebido de credenciales que permitían acceder a servidores administrados por un proveedor externo de monitoreo, evidenciando riesgos críticos derivados de la terciarización⁵⁰.

Un patrón similar se observó en **Argentina** con el hackeo de un proveedor de servicios de mensajería SMS, encargado de enviar códigos de verificación (OTP por sus siglas en inglés) y mensajes asociados a autenticación y recuperación de cuentas⁵¹. Al comprometer esta pasarela de mensajería SMS, los atacantes pudieron interceptar tráfico SMS en tiempo real, incluyendo códigos OTP. Esto facilitó el secuestro de cuentas mediante procesos de reseteo de contraseñas y otros flujos que dependen de verificación por SMS, reduciendo la efectividad del segundo factor cuando se basa en mensajes de texto.

El monitoreo regional también identificó filtraciones producidas a partir del **uso abusivo de accesos legítimos** mediante credenciales con autorización formal, sin que pudiera determinarse si las acciones fueron realizadas por sus titulares o por terceros que obtuvieron acceso a dichas cuentas. En **Perú**, la exposición de imágenes y datos personales almacenados en las bases del RENIEC⁵² fue atribuida al uso indebido de accesos asignados al Ministerio del Interior⁵³.

De forma similar, en **Ecuador** se investigó la filtración de datos del servicio de emergencias ECU 911 hacia empresas de servicios funerarios. Esto permitió que las mismas contactaran a familiares de personas en situación crítica incluso antes de que se produjera un fallecimiento, planteando cuestionamientos éticos y de protección de datos en contextos de vulnerabilidad⁵⁴.

Un conjunto especialmente preocupante de incidentes afectó a **instituciones públicas y servicios esenciales**, que expusieron la información de millones de personas. En **Paraguay**, dos filtraciones masivas —una del Tribunal Superior de

48. Contenedores de Azure: espacios de almacenamiento en la nube de Microsoft utilizados para guardar y gestionar archivos y datos. Si se configuran de forma incorrecta, pueden permitir el acceso no autorizado a información sensible.

49. El Testigo, “Una filtración de datos afecta a las instituciones financieras de América Latina, incluida República Dominicana”, El Testigo (Diciembre 4, 2024). Disponible en: <https://eltestigo.com/una-filtracion-de-datos-afecta-a-las-instituciones-financieras-de-america-latina-incluida-republica-dominicana>

50. Abel Cárdenas y Gianfranco Huamán, “El negocio ilegal de la información personal: la ruta detrás del robo de datos de Interbank”, Ojo Público (Noviembre 10, 2024). Disponible en: <https://ojo-publico.com/5390/ciberdelincuencia-la-ruta-detras-del-robo-datos-interbank>

51. Juan Brodersen, “Hackean un proveedor de mensajes de texto en Argentina y alertan sobre estafas: qué pasó y cómo protegerse”, Clarín (Marzo 30, 2025). Disponible en: https://www.clarin.com/tecnologia/hackean-proveedor-mensajes-texto-argentina-alertan-estafas-paso-protegerse_0_XqOTdOYj2B.html

52. Entidad estatal autónoma encargada de administrar la base de datos personales de ciudadanas y ciudadanos peruanos.

53. David Solar Silva, “Reniec niega hackeo masivo y denuncia al Mininter como responsable del uso indebido de datos”, Infobae (Abril 4, 2025). Disponible en: <https://www.infobae.com/peru/2025/04/04/reniec-niega-hackeo-masivo-y-denuncia-al-mininter-como-responsable-del-uso-indebido-de-datos/>

54. SWI swissinfo.ch, “Investigan una supuesta filtración de datos en Servicio de Emergencias de Ecuador ECU 911”, SWI swissinfo.ch (Junio 5, 2024). Disponible en: <https://www.swissinfo.ch/spa/investigan-una-supuesta-filtracion-de-datos-en-servicio-de-emergencias-de-ecuador-ecu-911/79794108>

Justicia Electoral, que involucró a más de 7 millones de personas, y otra de entidades financieras públicas con más de 17 mil registros— dejaron al descubierto datos altamente sensibles, incluyendo afiliación política, información laboral y salarios de personas funcionarias⁵⁵.

En **Uruguay**, se registraron múltiples filtraciones que afectaron a organismos estatales, entre ellas la exposición de casi 15 mil solicitudes de visa —correspondientes en su mayoría a personas migrantes y refugiadas—, bases de datos de atención ciudadana con más de 574 mil registros; y más de 13 mil credenciales de acceso a sistemas del Estado^{56 57 58}. En **Honduras**, por su parte, investigaciones periodísticas documentaron la circulación de datos del censo electoral y millones de números telefónicos en sitios de venta ilegal⁵⁹.

Las filtraciones que afectaron a sectores como **salud y educación** constituyen uno de los impactos más graves del período analizado. En **Argentina**, se pusieron a la venta más de 665 mil estudios médicos de pacientes que se atendieron en sanatorios y hospitales. Los datos van desde imágenes de radiografías, ecografías, tomografías, a pruebas en laboratorio⁶⁰. En **El Salvador**, se filtraron datos personales de casi un millón de personas afiliadas al sistema de seguro social, así como 50 GB de información proveniente de instituciones educativas y 141 GB de empresas de gestión de cobros^{61 62 63}. En **Chile**, un ataque de ransomware contra una universidad derivó en la publicación de 46 GB, incluyendo datos personales y financieros de estudiantes y personal universitario⁶⁴. En **México** y **Brasil**, ataques a instituciones educativas públicas expusieron datos de miles de estudiantes, en muchos casos personas con menos de 18 años, agravando los riesgos de infancias y adolescencias^{65 66}.

55. TEDIC, “Filtraciones masivas en Paraguay: cuando nuestros datos quedan a la deriva”, TEDIC (Marzo 31, 2025). Disponible en: <https://www.tedic.org/filtraciones2025/>

56. Pedro Tristant, “Filtración en Migraciones de Uruguay expuso 15 mil solicitudes de visa: en su mayoría cubanos y pakistaníes”, Infobae (Marzo 27, 2025). Disponible en: <https://www.infobae.com/america/america-latina/2025/03/27/filtracion-en-migraciones-de-uruguay-expuso-15-mil-solicitudes-de-visa-en-su-mayoria-cubanos-y-pakistanies/>

57. La diaria, “Ciberataque a Agesic: se filtran correos y números de teléfono de más de 574.000 registros”, la diaria (Febrero 11, 2025). Disponible en: <https://ladiaria.com.uy/politica/articulo/2025/2/agesic-detecto-la-filtracion-de-datos-de-su-servicio-de-atencion-a-la-ciudadania-y-realizara-analisis-forense-de-lo-sucedido/>

58. El Observador, “Intendencia de Paysandú sufrió ataque informático y hackers pidieron US\$ 650 mil para recuperar información”, El Observador (Julio 26, 2024). Disponible en: <https://www.elobservador.com.uy/ciencia-y-tecnologia/intendencia-paysandu-sufrio-ataque-informatico-y-hackers-pidieron-us-650-mil-recuperar-informacion-n5953207>

59. Mario Sánchez, “Datos de hondureños, de venta en sitios web clandestinos”, La Prensa (Junio 3, 2024). Disponible en: <https://www.laprensa.hn/premium/honduras-ciberseguridad-datos-hondurenos-venta-sitios-web-ro-bo-A19674958>

60. Juan Brodersen, “Hackean “Informe Médico”, un proveedor de software de Argentina y venden resultados de estudios de pacientes”, Clarín (Abril 4, 2025). Disponible en: https://www.clarin.com/tecnologia/hackean-proveedor-software-medico-argentina-venden-resultados-estudios-pacientes_0_HmJfY0ZYib.html

61. Silvia María Calderón López, “Filtración masiva de datos en El Salvador y la necesidad de contar medidas de ciberseguridad y regulación sobre protección de datos personales”, IPANDETEC (Septiembre 17, 2024). Disponible en: <https://www.ipandetec.org/el-salvador/filtracion-masiva-de-datos-en-el-salvador-y-la-necesidad-de-contar-medidas-de-ciberseguridad-y-regulacion-sobre-proteccion-de-datos-personales/>

62. David Bernal, “Hackers publican 39 gigabytes de información sustraída del ITCA-FEPADE”, La Prensa Gráfica (Enero 7, 2025). Disponible en: <https://www.laprensagrafica.com/elsalvador/Hackers-liberan-39-Gb-de-informacion-sustraída-del-ITCA-FEPADE-20250107-0094.html>

63. David Bernal, “Más datos personales de salvadoreños en línea, tras hackeo a una gestora de cobros”, La Prensa Gráfica (Abril 3, 2025). Disponible en: <https://www.laprensagrafica.com/elsalvador/Mas-datos-personales-de-salvadorenos-en-linea-tras-hackeo-a-una-gestora-de-cobros-20250402-0082.html>

64. Fabián Padilla, “Hackean a la U. Santa María y exponen miles de datos de alumnos en la dark web”, Fast Check (Noviembre 14, 2024). Disponible en: <https://www.fastcheck.cl/2024/11/14/hackean-a-la-u-santa-maria-y-exponen-miles-de-datos-de-alumnos-en-la-dark-web/>

65. Ignacio Gómez Villaseñor, “Ciberataque sin precedentes expone a escuelas públicas de México: ‘Peligra toda la red’”, Publimetro México (Abril 8, 2025). Disponible en: <https://www.publimetro.com.mx/noticias/2025/04/08/ciberataque-sin-precedentes-expone-a-escuelas-publicas-de-mexico-peligra-toda-la-red/>

66. Laís Martins, “Alagoas despeja dados de alumnos em site de empresa condenada”, Intercept Brasil (Agosto 13, 2024). Disponible en: <https://www.intercept.com.br/2024/08/13/governo-de-alagoas-despeja-dados-de-alunos-e-professores/>

De manera transversal, los incidentes registrados muestran que las filtraciones no se agotan en el momento inicial de la exposición de los datos. Por el contrario, suelen amplificarse a través de su **circulación y monetización en foros de la dark web**, donde la información es vendida o liberada masivamente. Durante el período analizado se documentó, por ejemplo, la venta de alrededor de 250 mil registros bancarios de personas en **Brasil** por montos equivalentes a pocos créditos dentro de estos mercados⁶⁷, así como la comercialización de credenciales de acceso a sistemas fiscales en **México** —incluyendo claves de firma electrónica— de al menos 111 mil contribuyentes⁶⁸.

En **Argentina** y **Venezuela**, se ofrecieron bases de datos de millones de registros personales, acompañadas de muestras parciales, conocidas como *samples*, que permiten a los compradores verificar la autenticidad de la información antes de adquirir los datos completos^{69 70}.

Este ecosistema de reventa **no se limita a foros especializados**. Se observó también una creciente compraventa de datos personales hacia plataformas de uso cotidiano, particularmente en Telegram. La investigación *Identidades en Venta: El mercado ilegal de compra y venta de datos personales latinoamericano en Telegram* de Derechos Digitales⁷¹ documentó el funcionamiento de grupos y canales en esta plataforma dedicados a la compra y venta ilegal de datos personales en distintos países de América Latina, donde direcciones, números de teléfono, información de salud, filiación política y otros datos sensibles circulan con facilidad y a bajo costo.

Los incidentes de filtraciones de datos muestran cómo la exposición reiterada de información personal ha tendido a normalizarse en la región, instalando una peligrosa **idea de inevitabilidad**. Sin embargo, detrás de cada base de datos filtrada no hay meros registros técnicos, sino personas cuyos derechos se ven comprometidos. Estos impactos no se distribuyen de manera homogénea: mujeres, infancias y adolescentes, personas LGBTIQ+, personas defensoras de derechos humanos y comunidades históricamente vulneradas enfrentan riesgos agravados de acoso, fraude, violencia digital y persecución cuando su información queda expuesta.

A nivel técnico, la aplicación de medidas como el mínimo privilegio, el cifrado de la información, la trazabilidad de accesos, la autenticación multifactor y la revisión periódica de qué datos se almacenan y por cuánto tiempo constituye además de una buena práctica, una obligación organizacional. Varias de estas medidas deben integrarse desde el desarrollo mismo de los sistemas, siguiendo el principio de privacidad

67. Felipe Payão, “Dados bancários de 250 mil brasileiros são vazados em fórum criminoso”, TecMundo: Tudo sobre Tecnologia, Entretenimento, Ciência e Games (Noviembre 27, 2024). Disponible en: <https://www.tecmundo.com.br/seguranca/400468-dados-bancarios-de-250-mil-brasileiros-sao-vazados-em-forum-criminoso.htm>

68. R3D, “Más de cien mil contraseñas de contribuyentes del SAT son filtradas en foros de la dark web”, R3D: Red en Defensa de los Derechos Digitales (Diciembre 19, 2024). Disponible en: <https://r3d.mx/2024/12/19/mas-de-cien-mil-contrasenas-de-contribuyentes-del-sat-son-filtradas-en-foros-de-la-dark-web/>

69. Daily Dark Web, “Massive Database Leak Reportedly Exposes 43 Million Records in Argentina”, Daily Dark Web (Enero 5, 2025). Disponible en: <https://dailydarkweb.net/massive-database-leak-reportedly-exposes-43-million-records-in-argentina/>

70. VE sin Filtro, “Usuarios de @MovistarVe sufrieron una grave filtración de datos personales”, [@vesinfiltro] (Abril 30, 2025). Disponible en: <https://x.com/vesinfiltro/status/1917532243846705173>

71. Derechos Digitales, “Identidades en venta: El mercado ilegal de compra y venta de datos personales latinoamericanos en Telegram”, Derechos Digitales (Marzo 11, 2026). Disponible en: <https://www.derechosdigitales.org/recursos/identidades-en-venta-el-mercado-ilegal-de-compra-y-venta-de-datos-personales-latinoamericanos-en-telegram/>

por diseño, según el cual la protección de datos no es un añadido posterior sino una consideración desde el origen.

3.4. Desinformación en elecciones

La desinformación se ha consolidado como una herramienta estratégica en los procesos electorales de América Latina. En contextos de polarización y urgencia informativa, la circulación de contenidos falsos o engañosos —en texto, imágenes, videos o audios— busca movilizar emociones para influir en el voto, favorecer o perjudicar candidaturas y erosionar la confianza en el proceso electoral. El monitoreo de procesos electorales en la región evidencia patrones que combinan **tácticas tradicionales e innovaciones tecnológicas**, convirtiendo la mentira organizada en un componente estructural de la competencia política. Durante este período ocurrieron elecciones en Brasil, Chile, Ecuador, México, Uruguay y Venezuela con tendencias que se presentan a continuación.

Una primera dinámica recurrente consiste en **sembrar dudas sobre la integridad del proceso electoral a partir de “pruebas” que aparentan ser técnicas** —pantallas, números, videos—, pero que en realidad están malinterpretadas o fuera de contexto. Quienes desinforman aprovechan el desconocimiento ciudadano sobre los procedimientos para presentar incidentes menores o errores humanos como si fueran evidencias de un fraude orquestado.

En **México**, por ejemplo, se viralizó que había “actas duplicadas” en el PREP⁷² como supuesta prueba de fraude, pese a que se trata de un conteo preliminar e informativo, sujeto a errores de captura o digitalización que se corrigen posteriormente en los cómputos oficiales⁷³. Narrativas similares ocurrieron en **Ecuador**, construidas a partir de “pruebas” visuales engañosas: se difundió un video que afirmaba que la autoridad electoral entregaba bolígrafos cuyo trazo se borraría para alterar votos. Sin embargo, el material correspondía a un video descontextualizado de otro país y otro año^{74 75}. En el escenario postelectoral, se viralizó una imagen que atribuía a la OEA la declaración de que los resultados no eran legales, pese a que un comunicado oficial validó el proceso⁷⁶.

Incluso caídas momentáneas de sitios institucionales —como las reportadas por el Instituto Electoral de la Ciudad de **México** durante la jornada y el desfase de actualización en el sitio del Servel⁷⁷ en **Chile**— fueron reinterpretadas como señales

72. El Programa de Resultados Electorales Preliminares (PREP) es un sistema informático implementado por las autoridades electorales que proporciona los resultados preliminares de una elección la misma noche de la jornada electoral, a partir del conteo rápido de las actas de escrutinio que llegan desde las casillas.

73. Regina López Puerta y Ave Velázquez, “Video desinforma sobre supuesto fraude electoral con actas duplicadas”, El Sabueso (Junio 11, 2024). Disponible en: <https://animalpolitico.com/verificacion-de-hechos/desinformacion/falso-fraude-electoral-actas-duplicadas>

74. Giuliana M. Andrade, “Es falso que el CNE entrega esferos que se borran”, LupaMedia (Abril 8, 2025). Disponible en: <https://lupa.com.ec/verificaciones/cne-esferos-borrables-elecciones-2025/>

75. Redacción Vistazo, “Correísmo denuncia en Fiscalía al CNE por “bolígrafos con tinta borrrable” que habrían perjudicado a Luisa González”, Vistazo (Mayo 29, 2025). Disponible en: <https://www.vistazo.com/politica/nacional/2025-05-29-revolucion-ciudadana-denuncia-fiscalia-cne-boligrafos-tinta-borrable-luisa-gonzalez-HF9412944>

76. Giuliana M. Andrade, “La OEA no reconoció que los resultados de las elecciones fueron ilegales”, LupaMedia (Abril 21, 2025). Disponible en: <https://lupa.com.ec/verificaciones/oea-reconoce-resultados-ecuador/>

77. El Servicio Electoral de Chile es un órgano autónomo del Estado, con rango constitucional, responsable de organizar, administrar y fiscalizar los procesos electorales y plebiscitarios.

de manipulación y usadas para sembrar dudas sobre la integridad del proceso^{78 79}.

En paralelo, aparece un patrón sostenido de **suplantación de identidad** mediante cuentas y piezas que imitan a medios para hacer que un rumor parezca noticia confirmada. En **Venezuela**, perfiles de Tiktok con estética de noticiero difundieron como hechos versiones no verificadas, como la supuesta detención o fuga del presidente del Consejo Nacional Electoral. La repetición en múltiples cuentas amplificó su visibilidad, generó confusión y luego fue aprovechada para desacreditar a la prensa independiente y reforzar narrativas oficialistas⁸⁰.

En **Ecuador**, el monitoreo identificó suplantación mediante piezas fabricadas que replicaban logos y estilos gráficos de medios e instituciones públicas para proyectar legitimidad. Con esa apariencia, se difundieron mensajes diseñados para activar miedo o indignación —por ejemplo, la falsa asociación entre migración y criminalidad o la oferta de becas inexistentes— en formatos visuales pensados para el consumo rápido, ya sea mediante publicidad pagada o capturas de pantalla diseñadas para viralizarse sin cuestionamientos⁸¹.

En esa misma lógica, circularon capturas falsas atribuidas a figuras políticas o videos reutilizados fuera de contexto para instalar narrativas o irregularidades inexistentes. En **Venezuela** se difundieron capturas falsas en X donde María Corina Machado felicitaba un intento de golpe de Estado en Bolivia⁸². En **México**, se reutilizó un video de 2021 donde una persona vota con un arma, como si correspondiera a la elección de 2024⁸³. En ambos casos, la apariencia de autenticidad bastó para que el contenido se viralizara antes de cualquier verificación, aprovechando la inmediatez del consumo en redes.

El salto cualitativo en la desinformación electoral llegó con **la masificación de herramientas de inteligencia artificial**, que permiten crear contenido hiperrealista a bajo costo y a una velocidad antes impensable. Las *deepfakes* —manipulaciones de video o audio que hacen parecer que una persona dijo o hizo algo que nunca ocurrió— se han vuelto especialmente efectivas porque transforman una narrativa falsa en una “prueba” audiovisual fácil de reenviar. En **Venezuela**, por ejemplo, circuló una *deepfake* en la que se superpuso una voz generada por IA sobre un video real de la dirigente Delsa Solórzano para hacerle decir que el candidato Edmundo

78. Cristóbal Palacios, “Lentitud en publicación de resultados: Servel informa desfase en actualización en su sitio web”, La Tercera (Octubre 28, 2024). Disponible en: <https://www.latercera.com/politica/noticia/servel-informa-desfase-en-actualizacion-de-resultados-electorales-en-su-sitio-web/INPDERXL4ZA4PNMADF43R5IHOA/>

79. Verificado, “Las desinformaciones que marcaron la jornada electoral en México 2024”, Verificado (Junio 4, 2024). Disponible en: <https://verificado.com.mx/desinformaciones-que-marcaron-jornada-electoral/>

80. Podcápsula Informativa, “Organizaciones internacionales reportan violaciones a los derechos humanos y digitales en Venezuela, mientras falsos noticieros en Tiktok posicionan rumores y facilitan propaganda oficialista”, Cazadores de Fake News (Octubre 21, 2024). Disponible en: <https://www.cazadoresdefakenews.info/organizaciones-internacionales-reportan-violaciones-a-los-derechos-humanos-y-digitales-en-venezuela-mientras-falsos-noticieros-en-tiktok-posicionan-rumores-y-facilitan-propaganda-oficialista/>

81. Lupa Media, “Desinformación a la carta: así se manipuló la campaña electoral en Ecuador”, Lupa Media (Abril 9, 2025). Disponible en: <https://lupa.com.ec/explicativos/desinformacion-electoral-ecuador-2025/>

82. Mardylid Castillo, “María Corina Machado no felicitó a las Fuerzas Armadas de Bolivia tras intento de golpe de Estado”, Cotejo.info (Julio 12, 2024). Disponible en: <https://cotejo.info/2024/07/fb-falso-maria-corina-machado-no-felicito-a-las-fuerzas-armadas-de-bolivia-tras-intento-de-golpe-de-estado/>

83. Verificado, “Las desinformaciones que marcaron la jornada electoral en México 2024”, Verificado (Junio 4, 2024). Disponible en: <https://verificado.com.mx/desinformaciones-que-marcaron-jornada-electoral/>

González “jamás ganó” las elecciones⁸⁴. También se difundieron audios presentados como “filtraciones” de WhatsApp atribuidos a María Corina Machado, que tras ser verificados, resultaron ser falsos y elaborados con IA⁸⁵.

En **Brasil**, la desinformación adoptó un sesgo de género explícito. Se documentaron al menos cinco ataques con deepfakes contra candidatas: imágenes o videos falsos donde se inserta el rostro de una mujer en cuerpos desnudos para generar contenido sexual⁸⁶. Este contenido busca degradar e intimidar, conectando directamente la desinformación con violencia de género en el ámbito político.

Al mismo tiempo, los casos muestran que **la desinformación suele operar de manera coordinada a través de múltiples plataformas**⁸⁷. En **Brasil**, un estudio sobre grupos políticos de extrema derecha durante la campaña municipal de 2024 encontró que 17% de los enlaces compartidos en WhatsApp contenían desinformación, frente a 7% en Telegram⁸⁸. En **Venezuela**, se documentaron redes de cuentas que se citan entre sí y simulan ser oposición para amplificar narrativas en X y TikTok, mientras que otras capas de la operación utilizan Telegram para el hostigamiento coordinado⁸⁹. Esta lógica alcanzó mayor sofisticación en **Ecuador**, donde se sumó la pauta pagada: empresas registradas en Estados Unidos habrían utilizado productos de Google para difundir anuncios desinformativos contra candidaturas⁹⁰.

3.5. Ataques dirigidos

Los ataques dirigidos consisten en acciones deliberadas contra infraestructuras, sistemas o servicios digitales específicos, y se caracterizan por no operar “al azar”, sino por seleccionar objetivos previamente identificados y desplegar acciones destinadas a cumplir un propósito determinado, como obtener acceso, interrumpir servicios, extorsionar o cometer fraude. En esta sección se describen distintas modalidades de ataques dirigidos identificadas en la región, como campañas de phishing, secuestro de cuentas, fraude mediante aplicaciones y ataques contra infraestructuras digitales.

84. Edy Pérez Alvarado, “Está alterado el video donde Delsa Solórzano dice que Edmundo González Urrutia ‘jamás ganó las elecciones’”, Cotejo.info (Diciembre 4, 2024). Disponible en: <https://cotejo.info/2024/12/fb-alterado-el-video-donde-delsa-solorzano-dice-que-edmundo-gonzalez-urrutia-jamas-gano-las-elecciones/>

85. Mardylid Castillo, “Falso audio de María Corina Machado en el que ofende a Delsa Solórzano”, Cotejo.info (Junio 4, 2024). Disponible en: <https://cotejo.info/2024/06/fb-falso-audio-de-maria-corina-machado-en-el-que-ofende-a-delsa-solorzano/>

86. Matheus S. Cruz, et al., “AI in the 2024 Brazilian Elections”, Aláfia Lab and Data Privacy Brasil (Noviembre, 2024). Disponible en: <https://desinformante.com.br/wp-content/uploads/2024/11/AI-in-the-2024-brazilian-elections.pdf>

87. Anna Bentes, “Elecciones, derechos digitales y desinformación: desafíos y aprendizajes a partir de la experiencia brasileña en 2022”, Derechos Digitales (Noviembre, 2023). Disponible en: <https://www.derechosdigitales.org/recursos/elecciones-derechos-digitales-y-desinformacion-desafios-y-aprendizajes-a-partir-de-la-experiencia-brasileña-en-2022/>

88. Redação Desinformante, “Pesquisa aponta que desinformação circula mais em grupos de extrema direita no WhatsApp que no Telegram”, desinformante (Enero 28, 2025). Disponible en: <https://desinformante.com.br/desinformacao-grupos-direita/>

89. Podcápsula Informativa, “Infiltrar, robar datos, estigmatizar y atacar, la ofensiva informativa del gobierno de Maduro contra la oposición”, Cazadores de Fake News (Agosto 26, 2024). Disponible en: <https://www.cazadoresdefakenews.info/organizaciones-internacionales-reportan-violaciones-a-los-derechos-humanos-y-digitales-en-venezuela-mientras-falsos-noticieros-en-tiktok-posicionan-rumores-y-facilitan-propaganda-oficialista/>

90. Lupa Media, “Desinformación electoral en Ecuador”, Lupa Media (Abril 9, 2025). Disponible en: <https://lupa.com.ec/explicativos/desinformacion-electoral-ecuador-2025/>

Si bien estas técnicas se utilizan en distintos contextos, es importante señalar que las mismas herramientas y vectores de ataque pueden emplearse también contra activistas, periodistas, defensoras y defensores de derechos humanos u organizaciones de la sociedad civil. Comprender cómo operan estos ataques permite dimensionar los riesgos que enfrentan distintos actores en el entorno digital y los impactos que estos incidentes pueden tener en la vida cotidiana de las personas y el funcionamiento de instituciones clave.

La motivación económica sigue siendo uno de los principales impulsores de los ataques en la región. Los métodos se han diversificado y sofisticado, como lo ilustra la **proliferación de troyanos bancarios**⁹¹ diseñados para el entorno latinoamericano. Infranus, detectado principalmente en **México**, mutó de spyware⁹² a troyano bancario con una capacidad particular: modificar el portapapeles de la víctima para reemplazar silenciosamente el número de cuenta al que se intenta transferir dinero, desviando fondos hacia los criminales⁹³. En **Colombia**, campañas dirigidas contra organismos públicos y empresas utilizaron troyanos de administración remota distribuidos a través de correos de phishing⁹⁴ altamente personalizados que suplantaban a bancos y servicios de mensajería; al abrir el adjunto, se instalaba software capaz de registrar teclas, capturar pantallas y robar credenciales⁹⁵.

Otra modalidad en expansión es la de los **préstamos por aplicativo**, que combina ingeniería social⁹⁶ con extorsión y se sostiene en condiciones de vulnerabilidad económica. En **Ecuador**, el Centro de Autonomía Digital (CAD)⁹⁷ describe cómo esta modalidad crece al aprovechar la falta de empleo y crédito formal. Esas aplicaciones ofrecen préstamos rápidos mediante procesos de aprobación simplificados, pero una vez instaladas, solicitan permisos intrusivos —contactos, galería, ubicación, cámara y registros de llamadas— que luego se convierten en la base de la coerción. Tras el préstamo, imponen intereses abusivos y plazos imposibles; ante cualquier demora, comienzan las amenazas, difamación a través de contactos, y en algunos casos la intimidación mediante el uso de fotos personales o íntimas y el rastreo de ubicación, e incluso la generación de “deudas” adicionales no solicitadas⁹⁸.

91. Los troyanos bancarios son un tipo de malware que se instala de forma oculta en el dispositivo de la víctima con el objetivo de robar credenciales de acceso. Su nombre proviene de la analogía con el caballo de Troya, pues se presentan como programas legítimos para engañar y lograr su instalación.

92. El spyware es un tipo de malware que se instala de forma oculta en un dispositivo para recopilar información sobre una persona usuaria sin su conocimiento o consentimiento, como contraseñas, mensajes, ubicación o actividad en pantalla, y enviarla a terceros.

93. Fernando Tavella, “Infranus: un troyano bancario distribuyéndose en México”, welivesecurity (Septiembre 26, 2024). Disponible en: <https://www.welivesecurity.com/es/investigaciones/infranus-troyano-bancario-distribuyendose-mexico/>

94. El phishing es una técnica de engaño para obtener información confidencial (como credenciales de acceso o datos bancarios) haciéndose pasar por una entidad legítima o persona de confianza. Se ejecuta mediante comunicaciones falsas pero aparentemente oficiales, como correos electrónicos, mensajes de texto (smishing) o llamadas telefónicas (vishing), que dirigen a la víctima a sitios web fraudulentos diseñados para robar sus datos o infectar su dispositivo con malware.

95. Fernando Tavella, “Troyano Remcos busca robar información sensible de empresas y organismos de Colombia”, welivesecurity (Junio 4, 2024). Disponible en: <https://www.welivesecurity.com/es/investigaciones/troyano-remcos-roba-informacion-empresas-organismos-colombia/>

96. La ingeniería social es el conjunto de técnicas de manipulación para engañar a las personas y lograr que revelen información confidencial, realicen acciones específicas o concedan acceso a sistemas protegidos. A diferencia de los ataques puramente técnicos, la ingeniería social explota la confianza, el miedo, la curiosidad o la falta de conocimiento.

97. Centro de Autonomía Digital: <https://autonomia.digital/>

98. Álvaro Paredes, “Apps de Préstamos - Una Trampa Digital”, CAD - Centro de Autonomía Digital (Abril 4, 2024). Disponible en: <https://autonomia.digital/2025/04/04/loan-apps-a-digital-trap.html>

En **México**, el Consejo Ciudadano reportó más de mil aplicaciones de este tipo hasta 2024, varias activas en Google Play⁹⁹. En **Perú**, la Superintendencia de Banca y Seguros alertó sobre al menos 17 apps con el mismo esquema¹⁰⁰.

Por otro lado, la **suplantación de identidad** se consolidó como un eslabón crítico en la cadena de fraude digital. El phishing sigue siendo uno de los vectores más frecuentes. En **Honduras**, organizaciones indígenas y defensoras del territorio han sido objeto de campañas de phishing personalizado que suplantan la identidad de donantes internacionales para obtener agendas de trabajo y mapear redes de contacto, con el objetivo de facilitar la persecución física por actores no estatales y empresas extractivas¹⁰¹.

Este mismo vector es utilizado con fines de fraude económico: en **Chile**, mensajes sobre el vencimiento de puntos de un programa de fidelización popular en el sector de combustibles dirigían a un sitio casi idéntico al oficial que solicitaba datos bancarios para un supuesto costo de envío¹⁰²; en **Colombia**, una maniobra similar suplantó a la Dirección de Impuestos y Aduanas Nacionales (DIAN) con falsos avisos de deuda¹⁰³. Este tipo de engaños se ve reforzado por el uso de IA, que permite producir mensajes más personalizados y verosímiles, reduciendo la efectividad de señales tradicionales de detección.

Cuando el engaño logra obtener credenciales, el robo de cuentas se convierte en una herramienta para escalar la estafa. En **República Dominicana**, la lista de víctimas incluye al presidente Luis Abinader, cuyo perfil de X fue vulnerado, además de ministros y el presidente del Senado; en distintos casos, los atacantes usaron las cuentas para solicitar dinero a contactos aprovechando la confianza asociada a la identidad suplantada¹⁰⁴. En **Honduras**, una banda utilizaba phishing para acceder a cuentas de WhatsApp y luego ofrecía dólares a precios bajos; las víctimas transferían dinero a cuentas controladas por los estafadores¹⁰⁵.

Una técnica más compleja es el *SIM swapping*, que explota la debilidad de la verificación por SMS para suplantar la identidad de una persona ante su operadora de telefonía y transferir su número a una tarjeta SIM controlada por el atacante, obteniendo así acceso a los códigos de verificación que protegen cuentas bancarias y otros servicios. En **Brasil**, una organización criminal habilitó más de 180

99. Secretaría de Seguridad y Protección Ciudadana, “LA SSPC ALERTA A LA CIUDADANÍA A TOMAR PRECAUCIONES PARA EVITAR SER VÍCTIMA DE PRÉSTAMOS “MONTADEUDAS” EN APLICACIONES MÓVILES”, gob.mx (Enero 28, 2025). Disponible en: <http://www.gob.mx/sspc/prensa/la-sspc-alerta-a-la-ciudadania-a-tomar-precauciones-para-evitar-ser-victima-de-prestamos-montadeudas-en-aplicaciones-moviles>

100. SBS, “SBS advierte a la población sobre nuevos aplicativos de préstamos fraudulentos”, Superintendencia de Banca, Seguros y AFP (Agosto 22, 2024). Disponible en: <https://www.sbs.gob.pe/>

101. Fundación Acceso, “Observatorio Centroamericano de Seguridad Digital: Informe interanual 2020-2025 [Manuscrito en preparación].

102. Génesis Friz, “‘Tus puntos van a caducar’: Phishing, la tentadora estafa que llega por SMS y cómo no caer en ella”, BioBioChile (Abril 7, 2025). Disponible en: <https://www.biobiochile.cl/noticias/nacional/denuncias/2025/04/07/tus-puntos-van-a-caducar-phishing-la-tentadora-estafa-que-llega-por-sms-y-como-no-caer-en-ella.shtml>

103. David Garzón, “Se hacen pasar por la Dian, no se deje estafar: en temporada de pago de impuestos aumenta el phishing”, Infobae (Agosto 24, 2024). Disponible en: <https://www.infobae.com/colombia/2024/08/24/se-hacen-pasar-por-la-dian-no-se-deje-estafar-en-temporada-de-pago-de-impuestos-aumenta-el-phishing/>

104. Pedro Martínez Sánchez, “Siguen los hackeos a las cuentas de WhatsApp de funcionarios y figuras”, Diario Libre (Julio 9, 2024). Disponible en: <https://www.diariolibre.com/actualidad/nacional/2024/07/08/siguen-hackeos-a-las-cuentas-de-whatsapp-de-funcionarios/2780756>

105. El País, “Así operaba banda de ciberataque de WhatsApp en Honduras”, Diario El País (Octubre 14, 2024). Disponible en: <https://www.elpais.hn/asi-operaba-la-banda-de-ciberataque-a-cuentas-de-whatsapp-en-honduras/>

chips con datos de terceros para transferir la titularidad de las líneas, acceder a cuentas bancarias y realizar transferencias fraudulentas¹⁰⁶. En **Costa Rica** se registró un precedente legal: la Superintendencia de Telecomunicaciones ordenó a Claro indemnizar a un cliente víctima de SIM swapping al establecer que la operadora incumplió su obligación de verificar la identidad de quien solicitó la reposición del chip¹⁰⁷. La resolución coloca en el centro del debate la responsabilidad de las empresas de telefonía en la protección de sus clientes, más allá de la prestación del servicio.

Paralelamente, una oleada de incidentes golpeó a **instituciones gubernamentales y servicios esenciales**, debilitando la capacidad del Estado para brindar atención y sostener operaciones. El *ransomware*¹⁰⁸ se consolidó como amenaza central en este terreno. En **Uruguay**, atacantes cifraron la información del gobierno departamental —incluidos respaldos— y exigieron 650 mil dólares en bitcoin, dejando servicios digitales inoperativos y forzando procesos de reconstrucción¹⁰⁹. En **Paraguay**, el Ministerio de Educación y Cultura sufrió un ataque que dejó fuera de servicio todos sus portales y trámites electrónicos, con los atacantes exigiendo un millón de dólares¹¹⁰. En **Argentina**, una empresa encargada de distribuir tarjetas de crédito y documentación oficial fue afectada por ransomware, con riesgo de exposición de datos personales¹¹¹.

También se registraron **incidentes con dimensiones políticas**. En **Bolivia**, la Agencia de Gobierno Electrónico registró cientos de ataques contra páginas estatales hacia fines de 2024 y uno de los episodios más visibles comprometió al sitio web de la Cámara de Senadores, cuya portada fue reemplazada por mensajes y simbología —ataque conocido como *defacement*^{112 113}—. En **Brasil**, el mismo día en que el juez Alexandre de Moraes ordenó el bloqueo de X, el Tribunal Supremo Federal y otras instituciones estatales sufrieron ciberataques simultáneos¹¹⁴. La coincidencia temporal y el hecho de que los ataques alcanzaran también al organismo

106. Assessoria de Comunicação – PCDF, “PCDF desarticula organização criminosa especializada no golpe do Sim Swap”, Polícia Civil do Distrito Federal (Febrero 12, 2025). Disponible únicamente desde Brasil o mediante una VPN con servidor ubicado en Brasil: <https://www.pcdf.df.gov.br/noticias/13572/pcdf-desarticula-organizacao-criminosa-especializada-no-golpe-do-sim-swap>

107. Adrián Z. Rivero, “Sutel ordena a Claro indemnizar por €6 millones a víctima de SIM swapping”, Semanario Universidad (Enero 10, 2025). Disponible en: <https://semanariouniversidad.com/pais/sutel-ordena-a-claro-indemnizar-por-%e2%82%a16-millones-a-victima-de-sim-swapping/>

108. El ransomware es un tipo de malware que bloquea el acceso a un sistema informático o cifra los archivos de la víctima, exigiendo el pago de un rescate (generalmente en criptomonedas) a cambio de liberarlos. Una vez infectado, el dispositivo muestra un mensaje en pantalla con las instrucciones para pagar, usualmente con una cuenta regresiva que aumenta la presión sobre la víctima.

109. El Observador, “Intendencia de Paysandú sufrió ataque informático y hackers pidieron US\$ 650 mil para recuperar información”, El Observador (Julio 26, 2024). Disponible en: <https://www.elobservador.com.uy/ciencia-y-tecnologia/intendencia-paysandu-sufrio-ataque-informatico-y-hackers-pidieron-us-650-mil-recuperar-informacion-n5953207>

110. Newsroom Infobae, “Ministerio de Paraguay alerta de ciberataque y pedido de un millón de dólares en bitcoins”, Infobae (Octubre 22, 2024). Disponible en: <https://www.infobae.com/americas/agencias/2024/10/22/ministerio-de-paraguay-alerta-de-ciberataque-y-pedido-de-un-millon-de-dolares-en-bitcoins/>

111. Juan Brodersen, “La empresa de logística OCASA sufrió un ciberataque de ransomware: la web está caída”, Clarín (Junio 21, 2024). Disponible en: https://www.clarin.com/tecnologia/empresa-logistica-ocasa-sufrio-ciberataque-ransomware-web-caida_0_AhR2VtSgrd.html

112. El defacement es un tipo de ataque que consiste en acceder sin autorización a un sitio web y modificar su contenido visible, reemplazando la página principal por imágenes y/o mensajes elegidos por el atacante.

113. Redacción El Deber, “Incrementan los hackeos a páginas del Estado y expertos advierten riesgos para la población”, El Deber (Agosto 17, 2024). Disponible en: https://eldeber.com.bo/pais/incrementan-los-hackeos-a-paginas-del-estado-y-expertos-advierten-riesgos-para-la-poblacion_381905

114. El Periodista, “Tribunal Supremo de Brasil sufrió ciberataque en medio de polémica por X”, El Periodista (Septiembre 3, 2024). Disponible en: <https://www.elperiodista.cl/2024/09/tribunal-supremo-de-brasil-sufrio-ciberataque-en-medio-de-polemica-por-x/>

encargado de ejecutar el bloqueo sugieren una acción coordinada en respuesta a la decisión judicial. En **Costa Rica**, el acceso no autorizado a un correo institucional de la Universidad de Costa Rica permitió enviar una amenaza de bomba que obligó a evacuar el campus¹¹⁵.

Los ataques dirigidos en la región demuestran que los principales blancos son las instituciones públicas y las empresas que manejan información sensible o servicios esenciales; por ello, también concentran una responsabilidad central en materia de seguridad digital. Cuando infraestructuras críticas o sistemas que gestionan datos fallan, los riesgos no se limitan al fraude económico, sino que pueden afectar la seguridad de las personas, el acceso a servicios y la capacidad de la ciudadanía —incluyendo periodistas, activistas y organizaciones sociales— para participar en la vida pública. En contextos donde organizaciones sociales y defensoras de derechos humanos dependen de estas plataformas para acceder a información pública o registrar denuncias, la interrupción de servicios también puede obstaculizar procesos de rendición de cuentas y acceso a derechos.

115. Erick Murillo, “UCR confirma que hackearon correo para enviar amenazas de bomba”, CR Hoy (Septiembre 30, 2024). Disponible en: <https://crhoy.com/tecnologia/ucr-confirma-que-hackearon-correos-para-enviar-amenazas-de-bomba/>

4. Áreas temáticas



4 Áreas temáticas

La presente sección es una sistematización de la información recopilada a partir de distintas fuentes y niveles de evidencia. Por un lado, integra insumos contruidos desde datos y documentación de casos; por otro, incorpora experiencias compartidas por organizaciones miembro del OLAD, así como patrones y preocupaciones comunes identificados a lo largo del trabajo conjunto del Observatorio durante el período cubierto por este informe.

El capítulo profundiza en cuatro áreas temáticas que emergieron con especial fuerza en la conversación regional y en los materiales revisados: la violencia de género facilitada por las tecnologías, la explotación de datos biométricos, los bloqueos de internet y la vigilancia.

A lo largo de las siguientes páginas, el análisis combina la evidencia cuantitativa con el conocimiento situado de las organizaciones, ofreciendo una visión panorámica, pero a la vez detallada de cómo estas amenazas se manifiestan en la vida de las personas y comunidades que defienden derechos en América Latina.

4.1. Violencia de género facilitada por las tecnologías

La violencia de género facilitada por las tecnologías (VGFT) es una de las amenazas más persistentes y en evolución en América Latina. Lejos de tratarse de episodios aislados, responde a un entramado de mecanismos que agresores —individuales o colectivos— utilizan para hostigar, controlar, humillar, sexualizar,

extorsionar o dañar a mujeres y personas LGTBQIA+ por razones vinculadas a su género o identidad, valiéndose de plataformas, dispositivos, sistemas algorítmicos y datos personales.

Durante el período que cubre este informe, organizaciones del OLAD documentaron tanto la persistencia de formas conocidas de agresión como la aparición de nuevas modalidades, que muestran la capacidad de los agresores para adaptarse a tecnologías recientes y a los contextos sociopolíticos de cada país. La expansión de herramientas de IA y los casos que alcanzaron visibilidad pública en distintos países confirman que esta violencia no es una suma de incidentes, sino un fenómeno estructural que se reinscribe en nuevas infraestructuras técnicas y escenarios sociales.

Las organizaciones que operan líneas de ayuda para víctimas de VGFT en la región — como el Centro S.O.S. Digital de Fundación InternetBolivia.org en Bolivia y Navegando Libres de Taller de Comunicación Mujer en Ecuador — han sido fundamentales para visibilizar las dinámicas de este tipo de violencia y, sobre todo, para brindar acompañamiento directo a las personas afectadas¹¹⁶.

4.1.1. Navegando Libres

En el caso de la línea de ayuda de Navegando Libres, los casos en Ecuador muestran la persistencia de formas conocidas de VGFT¹¹⁷. Tal es el caso de la extorsión sexual, difamación, difusión de contenido íntimo, acoso, suplantación de identidad y acceso no consentido a cuentas. Muchos de estos casos se vinculan a rupturas de pareja, conflictos familiares o represalias contra mujeres con activismo feminista y social.

Junto con estas manifestaciones recurrentes, la organización identificó formas emergentes particularmente graves. Una de ellas es la violencia facilitada por aplicaciones de préstamos: en un caso documentado, una mujer que solicitó un préstamo a través de una app fue víctima de acceso indebido a sus contactos sin su conocimiento y, ante retrasos en los pagos, tanto ella como sus familiares recibieron amenazas, mensajes intimidatorios y fotomontajes con contenido humillante.

Para la organización, este fenómeno debe entenderse en el contexto de precarización económica que afecta desproporcionadamente a las mujeres en Ecuador,

116. Para conocer más sobre el trabajo de estas organizaciones en materia de violencia de género facilitada por tecnologías, ver los recursos disponibles en: <https://tcmujer.org/> y <https://internetbolivia.org/>

117. Para conocer más detalles del concepto y formas de manifestación de la VGFT según los estándares internacionales de derechos humanos, ver: Derechos Digitales, *Combatir la violencia de género facilitada por tecnologías (VGFT) desde el enfoque del derecho internacional de los derechos humanos*. Disponible en: <https://www.derechosdigitales.org/recursos/combater-la-violencia-de-genero-facilitada-por-tecnologias-vgft-desde-el-enfoque-del-derecho-internacional-de-los-derechos-humanos/>

quienes enfrentan mayor desempleo y mayores cargas familiares y de cuidado, además de las brechas digitales de género que limitan su conocimiento sobre el funcionamiento de este tipo de aplicaciones y prácticas de seguridad digital.

También se reportaron varios casos donde agresores usaron la referencia a bandas criminales para aumentar el temor en situaciones de sextorsión, así como amenazas de exparejas con vínculos a empresas de seguridad estatal, lo que revela cómo la VGFT se entrelaza con estructuras de poder y acceso privilegiado a tecnologías de vigilancia.

A través del acompañamiento a una colectiva feminista, además, se documentó un caso de difusión masiva de contenido íntimo en grupos de Telegram. Integrantes de la colectiva intentaron infiltrarse y lograron identificar que uno de los pasos para pertenecer a estos grupos era compartir contenido sexual de mujeres familiares o conocidas. Tras esa exigencia, había otros mecanismos de verificación a los que no pudieron acceder por razones de seguridad, lo que sugiere una estructura organizada y escalonada para la difusión de este tipo de violencia.

El trabajo de documentación y acompañamiento también se ve afectado por decisiones de las plataformas. La suspensión temporal de la cuenta de Instagram de Navegando Libres —que la organización vincula con los cambios en las políticas de Meta¹¹⁸— evidencia cómo las plataformas pueden debilitar, por acción u omisión, infraestructuras de acompañamiento fundamentales para quienes atraviesan violencia digital.

4.1.2. S.O.S. Digital

En la misma línea, la evidencia cuantitativa del **Centro S.O.S. Digital** de Fundación InternetBolivia.org refuerza esta lectura regional y permite observar la magnitud del problema desde otra escala. La línea de ayuda registró 377 casos reportados de violencia digital en el período. El abuso sexual mediante TIC (29.5%) y el acoso (21%) fueron las formas más recurrentes de violencia, concentrando en conjunto cerca de la mitad de los casos.

Junto con ellas, también aparecen de manera sostenida otras manifestaciones de violencia como el desprestigio (10.5%), el crackeo (10%), el abuso de información (9.5%), las amenazas (9.5%) y el fraude (7%). Esto muestra que la VGFT no se limita a un solo repertorio de agresión, sino que suele desplegarse a través de formas múltiples y combinadas.

Los casos muestran además que las mujeres continúan siendo las principales

118. A lo largo de 2025, Meta implementó modificaciones en sus políticas de moderación que afectaron especialmente contenidos relacionados con género, diversidad sexual y educación sexual, lo que derivó en suspensiones y restricciones a cuentas de organizaciones feministas y de derechos humanos en varios países de la región.

afectadas, y que la mayor concentración de casos se ubica en el grupo de 25 a 54 años, seguido por 18 a 24 años y, en menor medida, por adolescentes de 13 a 17 años. Este patrón sugiere que, aunque la violencia digital afecta a distintos grupos etarios, tiene una incidencia particularmente fuerte sobre mujeres jóvenes y adultas en etapas de alta exposición social, laboral, afectiva y comunitaria.

Otro elemento relevante es que la respuesta de la línea de ayuda no se reduce a una dimensión técnica. A lo largo del período, las acciones más frecuentes fueron la contención emocional, la orientación legal y la orientación tecnológica, con un peso ligeramente mayor de la primera. Este dato es importante porque muestra que la VGFT produce daños que no pueden ser abordados únicamente desde aspectos técnicos de seguridad digital o gestión de plataformas; exige también respuestas jurídicas y de acompañamiento sostenido.

4.1.3. Otros casos

Más allá del trabajo de las organizaciones del OLAD, se identificaron casos de VGFT en fuentes públicas de distintos países. El primero es la circulación y ampliación de discursos misóginos en plataformas digitales, muchas veces impulsados por dinámicas algorítmicas. En **Brasil**, una investigación de Núcleo y AzMina mostró cómo TikTok expone progresivamente a adolescentes varones a contenidos de extrema derecha y narrativas que degradan a las mujeres¹¹⁹. En el mismo país, Brasil Paralelo impulsó en Meta una campaña masiva de publicidad antiaborto que combina segmentación, apelaciones emocionales y una agenda ultraconservadora que también alcanza cuestiones de género y diversidad sexual¹²⁰.

Un segundo patrón es la persistencia de la violencia sexual digital como mecanismo de coerción, humillación o chantaje. Esta lógica aparece en los casos de sextorsión reportados en aplicaciones de citas en **México**, donde los agresores construyen una relación de confianza inicial para luego amenazar con difundir imágenes íntimas y obtener dinero¹²¹. También se observa en **Ecuador**, en el caso de un hombre acusado de contactar por WhatsApp a una adolescente para solicitarle archivos sexuales tras escalar progresivamente el tono de los mensajes¹²².

Un tercer patrón, especialmente preocupante, es el uso de IA para sexualizar, desacreditar o exponer a mujeres sin su consentimiento. En **Bolivia**, los ataques contra mujeres en política incluyeron insultos sobre el cuerpo, insinuaciones sexuales y

119. Flávia Santos y Sofia Schurig, "Como o TikTok alimenta a misoginia entre adolescentes brasileiros", Núcleo Jornalismo (Abril 3, 2025). Disponible en: <https://nucleo.jor.br/reportagem/2025-04-03-tiktok-misoginia-adolescentes/>

120. Paulo Motoryn, "Brasil Paralelo já gastou meio milhão de reais em anúncios contra aborto", Intercept Brasil (Junio 21, 2024). Disponible en: <https://www.intercept.com.br/2024/06/21/brasil-paralelo-ja-gastou-meio-milhao-de-reais-em-anuncios-contra-aborto/>

121. Sharon Mercado, "Sextorsión aumenta 65% en aplicaciones de citas en febrero; Facebook Parejas encabeza la lista", El Universal (Febrero 12, 2025). Disponible en: <https://www.eluniversal.com.mx/nacion/sextorsion-aumenta-65-en-aplicaciones-de-citas-en-febrero-facebook-parejas-encabeza-la-lista/>

122. Lizette Abril, "Un hombre detenido por ciberacoso a una adolescente en Ecuador", Telemazonas (Noviembre 6, 2024). Disponible en: <https://www.telemazonas.com/hombre-detenido-ciberacoso-adolescente-ecuador/>

deepfakes destinados a erosionar su legitimidad pública¹²³. En **México**, esta misma dinámica afectó a figuras públicas como una senadora y una streamer, mediante la difusión de deepfakes sexuales sin su consentimiento^{124 125}. Y en **Chile**, un estudiante fue acusado de crear deepfakes sexuales de sus compañeras, lo que evidencia hasta qué punto estas herramientas ya se encuentran disponibles y pueden ser utilizadas para producir daño sin requerir conocimientos técnicos avanzados¹²⁶.

Este último patrón conecta de manera directa con los hallazgos de una **investigación sobre aplicaciones deepfake en América Latina**. A partir de una recolección automatizada de datos en Google Play se identificaron 105 aplicaciones disponibles a diciembre de 2024. El estudio concluyó que 89.5% de estas apps representan un potencial peligro para las mujeres¹²⁷.

Los hallazgos muestran que estas herramientas no son difíciles de encontrar ni usar. Por el contrario, plataformas como Google Play legitiman este ecosistema al permitir la circulación masiva de tecnologías que facilitan agresiones simbólicas y sexuales sin consentimiento, bajo esquemas comerciales lucrativos. A esto se suma su fácil uso, la presencia de imágenes promocionales sexualizadas, clasificaciones de edad engañosas y una falta de transparencia generalizada sobre la procedencia de muchas de estas aplicaciones. Este ecosistema es el resultado de decisiones comerciales que priorizan la rentabilidad sobre la seguridad de las mujeres y personas LGBTIQ+, y que convierten a las plataformas en cómplices de la violencia de género.

4.2. Explotación de datos biométricos

La explotación de datos alude a contextos en los que la información personal de las personas, especialmente cuando se trata de datos sensibles, deja de ser solo un dato sobre ellas y pasa a convertirse en un recurso del que otros obtienen beneficios económicos o estratégicos. No se trata únicamente de que una empresa recopile información, sino de preguntarse bajo qué condiciones lo hace, qué obtiene a cambio, cuánto comprenden las personas sobre ese tratamiento y si conservan algún margen para decidir o, más adelante, para recuperar el control sobre sus datos.

123. Marcelo Blanco, “Insultos, montajes y amenazas: La guerra silenciosa contra las mujeres en la política boliviana”, Bolivia Verifica (Abril 25, 2025). Disponible en: <https://boliviaverifica.bo/insultos-montajes-y-amenazas-la-guerra-silenciosa-contra-las-mujeres-en-la-politica-boliviana/>

124. Paola Alín, “El ‘caso Andrea Chávez’: la impunidad de la violencia digital contra las mujeres (ahora con inteligencia artificial)”, El País México (Octubre 16, 2024). Disponible en: <https://elpais.com/mexico/2024-10-16/el-caso-andrea-chavez-la-impunidad-de-la-violencia-digital-contra-las-mujeres-ahora-con-inteligencia-artificial.html>

125. Ignacio Izquierdo, «Alana Flores es víctima del “deepfake” y anuncia acciones legales contra usuario», infobae, 27 de mayo de 2025, <https://www.infobae.com/mexico/2025/05/27/alana-flores-es-victima-del-deepfake-y-anuncia-acciones-legales-contra-usuario/>

126. Génesis Friz y Valeska Belmar, “Acusan a alumno de 8° básico de crear imágenes sexuales de compañeras con IA en San Pedro de la Paz”, BioBioChile (Abril 25, 2025). Disponible en: <https://www.biobiochile.cl/noticias/nacional/region-del-bio-bio/2025/04/25/acusan-a-alumno-de-8-basico-de-crear-imagenes-sexuales-de-companeras-con-ia-en-san-pedro-de-la-paz.shtml>

127. Ximena Cuzcano-Chavez y Constanza González-Véliz, “Análisis del abuso de aplicaciones deepfake y su impacto en la violencia digital de género en América Latina y el Caribe”, Veritas (2025), n.o 61: 32-67, <https://doi.org/10.4067/s0718-92732025000200032>

Cuando lo que está en juego son datos biométricos, el problema adquiere una dimensión aún más delicada. A diferencia de una contraseña, el iris, el rostro o las huellas no pueden modificarse si son comprometidos, y su tratamiento puede tener efectos duraderos.

El caso de World, antes Worldcoin, permite observar esta problemática. Para entender las respuestas institucionales que se describen más adelante, es necesario remontarse brevemente a lo ocurrido en 2023. A partir de ese año, en varias ciudades de **Argentina** comenzaron a formarse largas filas frente a dispositivos que escaneaban el iris de quienes se acercaban. A cambio, la empresa ofrecía el equivalente a entre 30 y 50 dólares en criptomonedas¹²⁸. En agosto de ese año, 9.500 personas argentinas registraron su iris en un solo día (una persona cada nueve segundos) en medio de una inflación que superaba el 115% anual¹²⁹.

El fenómeno se repitió en otros países de la región con economías bajo presión como Ecuador, Chile, Perú, Colombia y República Dominicana¹³⁰. Detrás de esas filas estaba Worldcoin, un proyecto cofundado por Sam Altman, también fundador de OpenAI¹³¹, cuya implementación en América Latina quedó a cargo de la empresa Tools for Humanity (TFH). El proyecto ofrece una identidad digital basada en el escaneo del iris, con la promesa de crear un sistema global que permita distinguir humanos de bots en internet. A partir de ese caso, esta sección examina cómo los datos biométricos pueden convertirse en una fuente de valor para las empresas, y por qué esto ha encendido alertas en autoridades, tribunales y organizaciones de la sociedad civil.

World funciona a partir de dos momentos: el registro y el uso posterior de la identidad digital. Durante el registro, la persona descarga la World App y proporciona datos como nombre, teléfono, correo electrónico, cuenta bancaria y metadatos del dispositivo. Luego, debe acudir presencialmente a un dispositivo llamado *Orb*, que escanea su iris para completar la verificación. A partir de esas imágenes, el sistema genera un código de iris —una representación numérica de la textura del iris— y lo compara con códigos previos para comprobar si esa persona ya se registró antes. Si el código es único, se crea una credencial digital llamada *World ID*¹³².

La empresa sostiene que no conserva la imagen del iris como fotografía, sino que la transforma en códigos y fragmentos¹³³ para reducir su exposición directa. Sin

128. York Perry, "Worldcoin bate récord en Argentina pese a los riesgos y 9.500 personas se registran en un día", FayerWayer (Septiembre 5, 2023). Disponible en: <https://www.fayerwayer.com/internet/2023/09/05/worldcoin-bate-record-en-argentina-pese-a-los-riesgos-y-9500-personas-se-registran-en-un-dia/>

129. Hannah Pérez, "Worldcoin se vuelve popular en Argentina: 9.500 usuarios se registraron en un día", Diario Bitcoin (Agosto 31, 2023). Disponible en: <https://www.diariobitcoin.com/argentina/worldcoin-record-argentina-9-500-registros-dia/>

130. Pedro Martín Sánchez, "El caso de Worldcoin y la alerta de las autoridades con criptomonedas", Diario Libre (Noviembre 16, 2024). Disponible en: <https://www.diariolibre.com/economia/negocios/2024/11/16/el-caso-de-world-coin-y-la-alerta-de-las-autoridades-con-criptomonedas/2913636>

131. Wikipedia, "Worldcoin", Wikipedia, la enciclopedia libre (Abril 11, 2026). Disponible en: <https://es.wikipedia.org/w/index.php?title=Worldcoin&oldid=172924752>

132. Autoridade Nacional de Proteção de Dados, "Nota Técnica no 4/2025/FIS/CGF/ANPD: Tratamento de dados biométricos de usuários do Protocolo World ID no contexto do projeto Worldcoin", ANPD (Enero 23, 2025).

133. Estos códigos se conocen como IrisCode, representaciones binarias generadas a partir de los patrones únicos del iris mediante un algoritmo de codificación. A diferencia de una contraseña, este código no puede modificarse si es comprometido, ya que deriva directamente de un rasgo físico inmutable.

embargo, eso no elimina el problema de fondo: aunque la imagen no circule como foto, la biometría sigue siendo la base del sistema, porque de ella depende la verificación de unicidad. El dato cambia de forma, pero sigue siendo indispensable¹³⁴.

Una vez completado el registro, el uso de World ID ya no requiere un nuevo escaneo. Según la empresa, el sistema utiliza herramientas criptográficas para que la persona pueda demostrar que pertenece al conjunto de personas verificadas sin revelar nuevamente su biometría ni su identidad civil. La promesa del proyecto es justamente esa: permitir que alguien pruebe que es un “humano único” en distintos servicios digitales sin volver a exponer el dato biométrico original¹³⁵.

Para reforzar esa promesa de privacidad, incorporan mecanismos como fragmentación de datos, cómputo multipartito seguro y pruebas de conocimiento cero (SMPC y ZKPs respectivamente, por sus siglas en inglés). En términos simples, estas técnicas buscan que ninguna parte del sistema tenga acceso completo al código de iris, y que ciertas verificaciones puedan realizarse sin revelar toda la información subyacente.

Esta arquitectura técnica no elimina, sin embargo, las tensiones de fondo. Una de ellas es el consentimiento: en varios países, el registro fue promovido mediante incentivos económicos, lo que vuelve compleja la idea de una decisión plenamente libre, sobre todo cuando quienes se registraban eran en su mayoría personas en situaciones de precariedad económica, dispuestas a entregar datos irremplazables a cambio de unos pocos dólares en criptomonedas. La pregunta no es solo si una persona aceptó, sino en qué condiciones lo hizo y cuánto entendía realmente sobre el tratamiento de su biometría.

Otra tensión tiene que ver con el riesgo a largo plazo. Incluso cuando la empresa promete anonimización o fragmentación, persiste la duda sobre qué significa realmente eliminar un dato biométrico una vez que fue capturado, transformado y vinculado a una credencial digital. A esto se suma un riesgo adicional derivado de la propia complejidad del sistema. Una auditoría técnica en marzo de 2025 identificó múltiples vulnerabilidades en los circuitos criptográficos de World, incluyendo fallos que podrían permitir a un atacante registrarse varias veces burlando el mecanismo de unicidad¹³⁶. Aunque la empresa resolvió los problemas más graves, la auditoría también advirtió sobre riesgos estadísticos no resueltos. La existencia de estas brechas refuerza la preocupación sobre la seguridad de un sistema que maneja datos irremplazables.

También persiste la pregunta sobre quién controla realmente esos datos y con qué fines. La promesa de que los datos “no se usan para otros fines” descansa en gran medida en afirmaciones empresariales y en mecanismos técnicos difíciles de auditar de forma independiente.

134. Autoridade Nacional de Proteção de Dados, “Nota Técnica no 4/2025/FIS/CGF/ANPD: Tratamento de dados biométricos de usuários do Protocolo World ID no contexto do projeto Worldcoin”, ANPD (Enero 23, 2025).

135. Ibid.

136. Least Authority, “Security Audit Report Worldcoin”, Least Authority (Marzo 7, 2025). Disponible en: <https://leastauthority.com/wp-content/uploads/2025/03/Least-Authority-Worldcoin-MPC-Circuit-Final-Audit-Report.pdf>

Estas tensiones no quedaron en el plano conceptual. En varios países de la región, el despliegue de World activó respuestas institucionales que permiten observar con mayor precisión los problemas del modelo. En **Brasil**, la Autoridad Nacional de Protección de Datos (ANPD) abrió una fiscalización formal sobre el tratamiento de datos biométricos realizado por World Foundation y TFH. La investigación puso el foco en la recolección de datos sensibles a gran escala y en la forma en que la empresa obtenía el consentimiento. El principal cuestionamiento fue que el registro se promovía mediante una compensación financiera en criptomonedas, lo que podía comprometer la libertad del consentimiento, especialmente por tratarse de datos sensibles y de difícil reversión. En enero de 2025, la ANPD ordenó suspender la compensación económica ofrecida y exigió, además, medidas de transparencia como la designación de un encargado de datos personales.

La empresa intentó modificar su modelo con un esquema de invitaciones, donde la recompensa ya no se vinculaba al propio escaneo sino al ingreso de nuevas personas. Pero las autoridades consideraron que los riesgos persistían y mantuvieron las restricciones, incluso con la posibilidad de multas diarias.

En **Chile**, durante 2024, el Servicio Nacional del Consumidor (SERNAC)¹³⁷ cuestionó la falta de información clara sobre los fines del tratamiento, los riesgos asociados y las entidades que podrían acceder a los datos, desplazando la discusión hacia los derechos del consumidor. Poco después, la Corte Suprema acogió un recurso de protección presentado por la madre de un adolescente cuyo iris fue escaneado¹³⁸. El tribunal ordenó eliminar el World ID del menor y todo registro de sus datos biométricos subrayando que, al tratarse de una persona con menos de 18 años, no existió consentimiento válido de sus representantes legales. La sentencia fue clara, ya que la empresa no debió recopilar esos datos sin verificar la edad y sin el consentimiento correspondiente.

A este escenario se suma una investigación de la Fundación Amaranta, que aporta una dimensión situada y de género¹³⁹. A partir de entrevistas, el estudio muestra que quienes entregaron su iris fueron mayoritariamente mujeres madres de familia con necesidades económicas urgentes. También revela que, en numerosos casos, las personas no comprendían qué hacía la empresa con sus datos, qué riesgos implicaba ese tratamiento ni qué tan posible era borrar luego esa información. El estudio confirma que el problema está atravesado por contextos de precariedad, desigualdades de género y asimetrías de información que debilitan la posibilidad de una decisión realmente libre.

Más allá de **Brasil** y **Chile**, el caso World también generó alertas en otros países de la región. En **Perú**, la empresa fue investigada por la ANPD en medio de un debate público sobre la seguridad de los datos biométricos y la legalidad del modelo

137. Es el organismo público chileno encargado de proteger y promover los derechos de las personas consumidoras, fiscalizando el cumplimiento de la normativa y pudiendo iniciar acciones judiciales en representación de sus intereses.

138. SERNAC, "SERNAC denuncia ante la Justicia a Worldcoin por recolección indebida de datos biométricos", Servicio Nacional del Consumidor (Agosto 28, 2024). Disponible en: <https://www.sernac.cl/portal/604/w3-article-81932.html>

139. Cecilia Ananías Soto, et al., "Venta de datos biométricos a Worldcoin en Chile: vulnerabilidades en un país al debe con la protección de datos", ONG Amaranta (Enero 2, 2025). Disponible en: <https://amarantas.org/wp-content/uploads/2025/01/ong-amaranta-datos-biometricos.pdf>

de escaneo de iris a cambio de criptomonedas^{140 141}. En **República Dominicana**, Pro Consumidor ordenó el cese de las operaciones al detectar posibles cláusulas abusivas en los contratos y problemas vinculados al deber de información, la ausencia de domicilio social local y el tratamiento de datos biométricos a cambio de un beneficio económico¹⁴². En **Ecuador**, el despliegue del proyecto también estuvo rodeado de cuestionamientos públicos y clausuras por falta de permisos, en un contexto en que organizaciones y especialistas advirtieron sobre la opacidad de las empresas aliadas y la fragilidad institucional para supervisar de manera efectiva este tipo de prácticas¹⁴³.

Lo que estos casos muestran es que, pese a su sofisticación técnica, el modelo de World deja abiertas preguntas centrales sobre la validez del consentimiento, el control efectivo de los datos, la jurisdicción aplicable y los riesgos asociados a una eventual vulneración de información biométrica. Detrás de cada iris escaneado hay una persona que no podía imaginar las consecuencias de ese intercambio.

4.3. Cortes de internet

Un corte de internet, también conocido como apagón de internet o bloqueo de internet, es una interrupción en el funcionamiento de la conectividad que impide el acceso total o parcial a la red en una zona determinada. Puede producirse por causas tanto intencionales como accidentales y afectar desde áreas locales, como una ciudad, hasta regiones más amplias, incluyendo países enteros. La duración de estos eventos es variable y puede extenderse desde minutos hasta varios días, dependiendo de su origen y magnitud¹⁴⁴.

A diferencia de los casos documentados en el capítulo de Censura, donde lo que se restringe son sitios o plataformas específicos, los cortes afectan la conectividad en sí misma. Sus consecuencias interrumpen el derecho a buscar y difundir información, limitan la libertad de expresión, dificultan el acceso a servicios básicos como salud y educación, y en contextos de emergencia pueden aislar a comunidades enteras en momentos en que más necesitan comunicarse.

Las causas pueden ser muy distintas. Los **cortes intencionales** son aquellos en que un actor, normalmente estatal, interrumpe (u ordena la interrupción) delibe-

140. Jordan Arce, “Fenómeno del escaneo de iris por dinero en el Perú: las dudas entorno a Worldcoin y por qué ya se le investiga”, Infobae (Junio 3, 2024). Disponible en: <https://www.infobae.com/peru/2024/06/03/fenomeno-del-escaneo-de-iris-por-dinero-en-el-peru-las-dudas-entorno-a-worldcoin-y-por-que-ya-se-le-investiga/>

141. ANPD, “MINJUSDH supervisa la recopilación de datos personales por Worldcoin”, Gob.pe (Junio 3, 2024). Disponible en: <https://www.gob.pe/institucion/anpd/noticias/965752-minjUSDH-supervisa-la-recopilacion-de-datos-personales-por-worldcoin>

142. Comunicaciones Pro Consumidor, “Pro Consumidor suspende las operaciones de Worldcoin en República Dominicana”, Pro Consumidor (Noviembre 15, 2024). Disponible en: <https://proconsumidor.gob.do/pro-consumidor-suspende-las-operaciones-de-worldcoin-en-republica-dominicana/>

143. Paola Carrillo, “WorldCoin abusó de nuestros datos biométricos, pero hay más”, La Barra Espaciadora (Septiembre 18, 2024). Disponible en: <https://labarraespaciadora.com/worldcoin-datos-biometricos/>

144. Coop La Lonja, “Corte De Internet: Ataque A La Libertad De Expresión”, Coop La Lonja (Enero 12, 2012). Disponible en: <https://cooplaLonja.com.ar/corte-de-internet/>

radamente la conectividad, generalmente para controlar el flujo de información durante protestas o procesos electorales. Los **cortes colaterales** ocurren cuando internet se cae como consecuencia de otro evento como una crisis energética, sin que nadie lo haya ordenado directamente, pero con el mismo efecto práctico sobre las personas. Un tercer tipo agrupa los casos en que la desconexión responde a años de **infraestructura deteriorada**, sin que haya un evento específico que los provoque.

Durante el período cubierto por este informe, América Latina registró casos de los tres tipos en Venezuela, Ecuador, Chile, Panamá, Cuba y Colombia. El análisis combina la documentación técnica de las organizaciones del OLAD —entre ellas Conexión Segura, a través de su iniciativa de monitoreo **VE Sin Filtro** en Venezuela, y Fundación Karisma, a través del **Observatorio de Bloqueos de Internet** (OBI) del K+Lab en Colombia— con una sistematización de casos públicos documentados por medios de comunicación e iniciativas de monitoreo global.

Entre los casos de **corte intencional** documentados en la región, destaca el de **Panamá**. En junio de 2025, el gobierno suspendió el acceso a internet y la telefonía móvil en la provincia de Bocas del Toro durante casi dos semanas, en respuesta a movilizaciones sociales contra una reforma al sistema de seguridad social¹⁴⁵. La medida se implementó en el marco de una declaración de estado de emergencia.

Un año antes, VE Sin Filtro documentó una caída de conectividad en **Venezuela** que afectó exclusivamente a CANTV y Movilnt las dos principales operadoras estatales, durante casi dos horas, dejando a varios estados sin señal¹⁴⁶. No hubo explicación oficial y aunque no es posible confirmar que fue intencional, ocurrió cuatro días después de las elecciones presidenciales del 28 de julio de 2024, en medio de una escalada de bloqueos a sitios web. La opacidad oficial ante este incidente es, en sí misma, parte de un patrón.

Los cortes colaterales en la región durante el período estuvieron marcados principalmente por crisis energéticas que arrastraron consigo la conectividad. **Ecuador** fue el primer país en enfrentarlos, ya que una severa sequía que afectó las centrales hidroeléctricas, responsables del 72% de la generación eléctrica nacional¹⁴⁷, desencadenó apagones que llegaron a las 14 horas diarias, dejando sin internet a varias provincias durante meses¹⁴⁸. En **Venezuela**, por su parte, un colapso del sistema eléctrico nacional el 30 de agosto de 2024 dejó al país sin conectividad durante casi 21 horas, donde 8 de cada 10 personas quedaron sin acceso a internet¹⁴⁹. El gobierno atribuyó el apagón a un sabotaje de la oposición, misma

145. Zach Rosson y Felicia Anthonio, "Rising repression meets global resistance: Internet shutdowns in 2025", Access Now (Marzo, 2025). Disponible en: <https://www.accessnow.org/wp-content/uploads/2026/03/KeepItOn-Internet-Shutdowns-2025-Annual-Report.pdf>

146. VE sin Filtro, "Redes de control: Censura y represión digital en las elecciones presidenciales en Venezuela", VE sin Filtro (2024). Disponible en: https://vesinfiltro.org/res/files/informe-presidenciales_2024-VEsinFiltro.pdf

147. Wikipedia, "Apagones de Ecuador de 2024", Wikipedia, la enciclopedia libre (Abril 5, 2026). Disponible en: https://es.wikipedia.org/w/index.php?title=Apagones_de_Ecuador_de_2024&oldid=172839309

148. Freedom House (2025), "Ecuador: Freedom on the Net 2025 Country Report", Freedom House (2025). Disponible en: <https://freedomhouse.org/country/ecuador/freedom-net/2025>

149. VE sin Filtro (2024), "Redes de control: Censura y represión digital en las elecciones presidenciales en Venezuela", VE sin Filtro (2024). Disponible en: https://vesinfiltro.org/res/files/informe-presidenciales_2024-VEsinFiltro.pdf

narrativa que se repetiría en los meses siguientes, cada vez que el sistema eléctrico volviera a colapsar¹⁵⁰.

Cuba concentró el mayor número de episodios en el período. Entre octubre de 2024 y marzo de 2025, el país experimentó cuatro colapsos del sistema eléctrico nacional que afectaron la conectividad. El primero, provocado por una falla en la central termoeléctrica, dejó a 10 millones de personas sin luz ni internet¹⁵¹. Le siguieron los daños del huracán Rafael en noviembre¹⁵², una nueva falla en diciembre y otra en marzo de 2025, todas responden a la misma causa: escasez de combustible e infraestructura obsoleta sin mantenimiento¹⁵³. **Chile** vivió su propio episodio cuando un fallo masivo en la red eléctrica dejó sin luz a 14 de las 16 regiones del país interrumpiendo internet y telefonía móvil por más de 12 horas en lo que fue el mayor apagón desde 2010¹⁵⁴.

En **Colombia**, OBI de Karisma documentó dos caídas en la provincia de Chocó, en agosto de 2024. La primera de entre 6 y 12 horas¹⁵⁵, coincidente con una tormenta torrencial que cortó el suministro eléctrico, y la segunda de entre 3 y 6 horas¹⁵⁶. Estos casos se inscriben además en un contexto de precariedad donde solo el 13% de la población tiene acceso a internet, principalmente en la capital departamental, lo que significa que cualquier interrupción golpea a una comunidad que ya de por sí tiene un acceso muy limitado.

Un tercer tipo de corte se manifiesta como desconexión progresiva por **deterioro de la infraestructura**. **Cuba** ilustra con claridad esta dinámica, pues entre octubre y diciembre de 2024, el país ocupó el último lugar mundial en velocidad de descarga con un promedio de 2.96 Mbps, siendo insuficiente incluso para tareas básicas como videollamadas o transmisión de video en calidad estándar que requieren al menos 10 Mbps¹⁵⁷. A mayo de 2025, la velocidad había mejorado apenas hasta 3.35 Mbps, manteniéndose entre los últimos puestos del índice global¹⁵⁸. Décadas de desinversión, agravadas por un bloqueo económico que ha limitado el acceso a tecnología y financiamiento externo, y la dependencia de una sola empresa estatal han derivado en una infraestructura obsoleta que no logra sostener una conectividad mínima para la población.

150. Wikipedia, "Apagones de Venezuela de 2024", Wikipedia, la enciclopedia libre (Febrero 22, 2026). Disponible en: https://es.wikipedia.org/wiki/Apagones_de_Venezuela_de_2024

151. Orlando González, "Cuba sufre apagón general y caída significativa del servicio de internet", Guardianes Digitales (Abril 21, 2024). Disponible en: <https://guardianesdigitales.blogspot.com/2024/10/cuba-sufre-apagon-general-y-caida.html>

152. Diktyon y IODA, "Cuba enfrenta apagones y cortes de internet tras falla de la red eléctrica nacional", IODA (Noviembre 27, 2024). Disponible en: <https://ioda.inetintel.cc.gatech.edu/reports/cuba-enfrenta-apagones-y-cortes-de-internet-tras-falla-de-la-red-electrica-nacional/>

153. Carla Gloria Colomé, "Un nuevo apagón deja a Cuba a oscuras en su peor crisis energética en décadas", El País América (Marzo 14, 2025). Disponible en: <https://elpais.com/america/2025-03-15/un-nuevo-apagon-deja-a-cuba-a-oscuras-en-su-peor-crisis-energetica-en-decadas.html>

154. The Associated Press, "A Sweeping Power Blackout Leaves Most of Chile in Darkness", Houston Public Media (Febrero 26, 2025). Disponible en: <https://www.houstonpublicmedia.org/npr/2025/02/26/g-s1-50785/a-sweeping-power-blackout-leaves-most-of-chile-in-darkness/>

155. K+Lab, "[MICRO-CAIDA] Reporte: Caída de Red - Quibdó, Chocó 1", Fundación Karisma (Noviembre 28, 2024). Disponible en: <https://obi.karisma.org.co/2024-10-28-colombia-microcaida-quirbo-choco-agosto-2/>

156. K+Lab, "[MICRO-CAIDA] Reporte: Caída de Red - Quibdó, Chocó 2", Fundación Karisma (Noviembre 28, 2024). Disponible en: <https://obi.karisma.org.co/2024-10-28-colombia-microcaida-quirbo-choco-agosto/>

157. Diktyon, "Censura de Internet en Cuba: Informe número 7", Diktyon (2024). Disponible en: https://github.com/diktyoncuba/public/blob/main/Informes/Informe-7_Oct-Dic-2024.pdf

158. Ookla, "Cuba's Mobile and Broadband Internet Speeds", Ookla (2025). Disponible en: <https://www.speedtest.net/global-index/cuba>

A esto se suma la restricción de paquetes ilimitados de internet en pesos cubanos para priorizar el pago en dólares estadounidenses a los servicios que implementa ETECSA¹⁵⁹ desde mayo de 2025, introduciendo paquetes en moneda extranjera y estableciendo límites al consumo en moneda nacional¹⁶⁰. El resultado es que cualquier plan de datos más allá del tope básico supera el salario mínimo mensual del país, convirtiendo la conectividad en un privilegio económico para quienes no tienen acceso a divisas¹⁶¹. **Cuba** no está desconectada de manera técnica, pero para quienes no tienen divisas, la diferencia con un corte en la práctica es mínima.

4.4. Vigilancia

La vigilancia digital es el monitoreo, interceptación, recolección y análisis de datos en línea realizados por actores estatales o privados con fines de control o neutralización de personas consideradas de interés¹⁶². En América Latina, esta práctica ha sido históricamente dirigida contra personas que defienden los derechos humanos, en continuidad con prácticas de vigilancia que nos atraviesan desde períodos coloniales. Lo que durante décadas operó a través de seguimientos físicos o interceptaciones telefónicas hoy se suma –sin reemplazarlos– a nuevas modalidades que se despliegan en los dispositivos de las personas, en el análisis de sus rostros y en el monitoreo de sus palabras en línea, muchas veces imperceptibles para quien las padece, lo que las convierte en herramientas eficaces de control y represión.

La vigilancia digital en América Latina se manifestó a través de varias modalidades que reflejan la expansión del control estatal sobre la vida de las personas en la región. Entre las tendencias documentadas destacan el uso de *spyware* contra periodistas y activistas; el acceso físico forzado a dispositivos durante detenciones u operativos policiales; el despliegue de sistemas de reconocimiento facial, video-vigilancia masiva y plataformas de análisis masivo de datos; y el ciberpatrullaje en redes sociales.

Durante el período cubierto por este informe, organizaciones del OLAD documentaron estos fenómenos desde distintos ángulos. **Fundación Acceso** investigó los efectos psicosociales del *spyware* sobre quienes lo han sufrido en Centroamérica y documentó a través del Observatorio Centroamericano de Protección Digital

159. Empresa de Telecomunicaciones de Cuba S.A (ETECSA)

160. Orlando González, “ETECSA Incrementará Tarifas y Dolarizará Servicios en 2025”, Guardianes Digitales (2025). Disponible en: <https://guardianesdigitales.blogspot.com/2024/12/etecsa-incrementa-tarifas-y-dolariza.html>

161. Carlos Cuevas, “¿Racionamiento de internet en Cuba? Precio de un plan de datos “extra” supera el salario mínimo”, Bloomberg Línea (Junio 6, 2025). Disponible en: <https://www.bloomberglinea.com/latinoamerica/racionamiento-de-internet-en-cuba-precio-de-un-plan-de-datos-extra-supera-el-salario-minimo/>

162. Rafael Bonifaz, “Herramientas de Vigilancia Digital identificadas en Centroamérica”, Fundación Acceso (2020). Disponible en: https://www.acceso.or.cr/wp-content/uploads/2021/08/2020_Art_Herramientas_Vigilancia_CA-mayo2020.pdf

tendencias críticas de vigilancia. Mientras que **Conexión Segura**, y su iniciativa de monitoreo VE Sin Filtro, registraron el despliegue de tecnologías de vigilancia en Venezuela durante el proceso electoral de 2024. A estos aportes se suman casos documentados por medios de comunicación, que permiten construir una imagen regional del fenómeno.

El uso de spyware acumuló nuevas evidencias durante este período. En **México**, documentos judiciales del litigio entre WhatsApp y la empresa israelí NSO Group —fabricante del spyware Pegasus— revelaron en abril de 2025 que 456 personas fueron atacadas con este software entre abril y mayo de 2019 durante el gobierno de Andrés Manuel López Obrador, convirtiéndolo en el país con más víctimas de un total de 1.233 identificadas a nivel global¹⁶³. La Secretaría de Defensa Nacional había suscrito un contrato para adquirir Pegasus en abril de ese mismo año, y el operador final del sistema sería el Centro Militar de Inteligencia, una agencia secreta cuya existencia ha sido negada reiteradamente por las propias fuerzas armadas.

En 2024, Estados Unidos confirmó haber financiado el uso de Pegasus en **Colombia** para operaciones contra el narcotráfico durante la administración de Iván Duque, pagando 11 millones de dólares¹⁶⁴. Si bien la versión oficial estadounidense sostuvo que Duque no fue informado, especialistas y una denuncia penal cuestionaron esa versión, señalando que un acuerdo de esa magnitud difícilmente podría haberse realizado sin conocimiento del Ejecutivo^{165 166}.

En **Ecuador**, la Asamblea Nacional resolvió en diciembre de 2024 iniciar un proceso de fiscalización ante denuncias de uso de Pegasus por parte del gobierno de Daniel Noboa para vigilar a periodistas, opositores y activistas, aunque al cierre de este informe dicho proceso no había arrojado resultados públicos¹⁶⁷.

163. R3D, “Gobierno mexicano usó Pegasus para espiar al menos a 456 personas en 2019”, R3D: Red en Defensa de los Derechos Digitales (Abril 14, 2025). Disponible en: <https://r3d.mx/2025/04/14/gobierno-mexicano-uso-pegasus-para-espiar-al-menos-a-456-personas-en-2019/>

164. WIRED, “Estados Unidos confirma que financió el uso del software espía Pegasus en Colombia”, WIRED (Noviembre 8, 2024). Disponible en: <https://es.wired.com/articulos/estados-unidos-confirma-que-financio-el-uso-del-software-espia-pegasus-en-colombia>

165. Julio Sánchez Cristo, “Expertos en ciberseguridad dicen que es casi imposible que Duque no supiera del software Pegasus”, Cambio Colombia (Noviembre 16, 2024). Disponible en: <https://cambio colombia.com/personajes/articulo/2024/11/es-casi-imposible-que-duque-no-supiera-del-software-pegasus-expertos-cuestionan-version>

166. Iván Cepeda Castro, “Senador Iván Cepeda denuncia al expresidente Iván Duque por presuntos delitos relacionados con la compra ilegal del software espía «Pegasus» y transferencias irregulares de fondos”, Iván Cepeda Castro (Septiembre 25, 2024). Disponible en: <https://ivancepedacastro.com/senador-ivan-cepeda-denuncia-al-expresidente-ivan-duque-por-presuntos-delitos-relacionados-con-la-compra-ilegal-del-software-espia-pegasus-y-transferencias-irregulares-de-fondos/>

167. Richard Josue Jimenez Mora, “Pegasus: la Asamblea fiscalizará supuesto espionaje del Gobierno”, Diario Expreso (Diciembre 17, 2024). Disponible en: <https://www.expreso.ec/actualidad/asamblea-pegasus-espionaje-224876.html>



Más allá de los números, detrás de cada tecnología de vigilancia hay personas que cargan con las consecuencias. Un estudio de **Fundación Acceso** publicado en abril de 2025 exploró, a través de entrevistas con personas defensoras y periodistas de **Centroamérica** infectadas con *spyware*, los impactos concretos de haber sido sometidas a este tipo de vigilancia¹⁶⁸. Las personas entrevistadas describieron impactos que comenzaban con pánico inicial y derivaban en estados prolongados de alerta constante, ansiedad, insomnio y depresión. Varias personas cambiaron de rutas, dejaron de frecuentar ciertos lugares, modificaron sus hábitos en redes sociales y migraron a aplicaciones de mensajería más seguras. Incluso, algunas terminaron en el exilio.

El impacto también se extendió a los equipos de trabajo, ya que cuando una persona revela que fue vigilada, se instala una cadena de pánico que obliga a destinar tiempo y recursos a la seguridad en lugar de al trabajo de defensa. A esto se suma un impacto económico como la compra de nuevos dispositivos, gastos en terapia psicológica, o costos de reubicación.

En ese contexto, Fundación Acceso desarrolló una guía de acompañamiento integral para personas que brindan atención en protección digital a quienes han sido afectadas por *spyware* y otras tecnologías de vigilancia¹⁶⁹.

En relación a Centroamérica, el Observatorio Centroamericano de Protección Digital¹⁷⁰, impulsado por Fundación Acceso, registró entre 2024 y 2025 varias tendencias críticas¹⁷¹. En **Guatemala** y **Nicaragua**, el acceso físico a dispositivos ha permitido a fiscalías y gobiernos construir narrativas de “conspiración” usando herramientas cifradas legítimas como supuesto indicio de criminalidad.

Específicamente, el gobierno de Daniel Ortega en **Nicaragua** ha consolidado una infraestructura que opera en múltiples capas. Desde 2017, en una base militar en Managua opera una infraestructura que combina radiogoniometría —capaz de localizar señales telefónicas— con el sistema SORM-3, que permite interceptar llamadas, mensajes, correos electrónicos, redes sociales y transacciones bancarias¹⁷². A eso se suma la persecución transnacional de exiliados en **Costa Rica** mediante *doxing* y monitoreo de redes sociales¹⁷³.

168. Olga Paz, “Estudio de impactos y afrontamientos psicosociales ante ataques digitales”, Fundación Acceso (Abril, 2025). Disponible en: https://pasalavoz.acceso.or.cr/Estudio_Impactos_psicosociales_spyware_FAcceso.pdf

169. José Luis Dardón Galicia, “Guía de acompañamiento integral para personas que brindan atención en protección digital a personas y organizaciones que han sido afectadas con *spyware* y otras tecnologías de vigilancia”, Fundación Acceso (Julio 30, 2025). Disponible en: <https://pasalavoz.acceso.or.cr/guia.html>

170. Registro y análisis sistemático de incidentes de seguridad digital que afectan a personas defensoras, periodistas y organizaciones de la sociedad civil en Centroamérica. Disponible en: <https://www.acceso.or.cr/observatorio-centroamericano-de-proteccion-digital/>

171. Fundación Acceso, “Observatorio Centroamericano de Seguridad Digital: Informe interanual 2020-2025 [Manuscrito en preparación]”

172. Redacción Confidencial, “Centro de espionaje ruso opera en base militar de Mokorón en Managua”, Confidencial (Agosto 26, 2024). Disponible en: <https://confidencial.digital/politica/el-centro-de-espionaje-de-rusia-en-el-cerro-mokoron-de-nicaragua/>

173. Fundación Acceso, “Observatorio Centroamericano de Seguridad Digital: Informe interanual 2020-2025 [Manuscrito en preparación]”.

En **Venezuela**, Conexión Segura documentó durante el proceso electoral el despliegue de distintas tecnologías de vigilancia¹⁷⁴. Identificaron una campaña de phishing dirigida a simpatizantes de la oposición mediante un formulario falso que recopilaba datos personales como la dirección. El enlace malicioso fue promovido a través de cuentas falsas en X, Instagram, TikTok y Telegram. Asimismo, se registró el uso de drones para capturar imágenes de manifestaciones con enfoque en los rostros de asistentes, posteriormente difundidas por voceros gubernamentales.

En paralelo, documentaron denuncias de revisión ilegal de teléfonos en operativos policiales, donde agentes exigían el desbloqueo de dispositivos para inspeccionar conversaciones de WhatsApp y buscar términos asociados a figuras políticas opositoras. A esto se sumó la instrumentalización de la aplicación estatal VenApp, originalmente diseñada para reportar fallas en servicios públicos, que fue utilizada para canalizar denuncias anónimas al gobierno contra manifestantes, mediante el envío de fotografías y datos de geolocalización, lo que permitía ubicar a las personas denunciadas.

A estas modalidades se suma la expansión de tecnologías de vigilancia en espacios públicos, **como la videovigilancia masiva y el reconocimiento facial**. En **Brasil**, São Paulo implementó a finales de 2024 el sistema Smart Sampa, una iniciativa de videovigilancia y reconocimiento facial con el objetivo declarado de identificar fugitivos y prevenir delitos mediante el cotejo en tiempo real de imágenes con bases de datos judiciales. Ha implicado la instalación de 40.000 cámaras en espacios públicos y privados a nivel municipal¹⁷⁵. Más del 8% de los arrestados por Smart Sampa debieron ser liberados por error: un jubilado de 80 años estuvo horas detenido porque el sistema lo identificó como un agresor sexual; un paciente psiquiátrico fue esposado en un centro de salud mental por una orden de arresto desactualizada. Organizaciones de la sociedad civil señalaron además que los datos oficiales no registran la identidad racial de más de la mitad de las personas detenidas, lo que impide evaluar si el sistema incurre en racismo algorítmico.

La expansión del sistema alcanzó también entornos educativos, pues cerca de 400 cámaras de Smart Sampa fueron instaladas en escuelas municipales de São Paulo, donde el reconocimiento facial opera en las áreas de acceso, generando registros biométricos de estudiantes, docentes y personal sin que existieran políticas de privacidad claras ni mecanismos de consentimiento informado para personas con menos de 18 años¹⁷⁶.

Son múltiples las iniciativas de despliegue de tecnologías de reconocimiento facial en **Brasil**. Entre ellas, se registraron la instalación de 17 puntos de búsqueda con reconocimiento facial en Río de Janeiro, durante la celebración de Año Nuevo 2024

174. VE sin Filtro, "Redes de control: Censura y represión digital en las elecciones presidenciales en Venezuela", VE sin Filtro (2024). Disponible en: https://vesinfiltro.org/res/files/informe-presidenciales_2024-VEsinFiltro.pdf

175. Agencia AFP, "Smart Sampa: La revolucionaria, pero polémica red de vigilancia digital en Sao Paulo", El Comercio (Marzo 17, 2026). Disponible en: <https://elcomercio.pe/mag/historias/smart-sampa-la-revolucionaria-pero-polemica-red-de-vigilancia-digital-en-sao-paulo-nnda-nnrt-noticia/>

176. InternetLab, "Tecnologias de Vigilância e Inteligência Artificial na Educação: Promessas de modernização, realidades de opacidade", InternetLab (Octubre, 2025). Disponible en: https://internetlab.org.br/wp-content/uploads/2025/10/relatorio_ia_28092025.pdf

en la playa Copacabana¹⁷⁷, y el despliegue de 12 cámaras adicionales de reconocimiento facial, drones y 18 puntos de control en las calles de acceso, durante el concierto gratuito de Lady Gaga en esa misma playa en mayo de 2025 al que asistieron más de 2,5 millones de personas^{178 179}.

En **Argentina**, el gobierno de Javier Milei creó la Unidad de Inteligencia Artificial Aplicada a la Seguridad, que habilita a las fuerzas federales a patrullar redes sociales y dark web, analizar imágenes de cámaras en tiempo real mediante reconocimiento facial, utilizar algoritmos para “predecir” delitos futuros, crear perfiles de sospechosos, y patrullar con drones áreas extensas¹⁸⁰. En mayo de 2025, el Plan de Inteligencia Nacional reveló que la Secretaría de Inteligencia de Estado tenía como objetivo monitorear a actores que generaran “pérdida de confianza en políticas económicas” o “manipularan la opinión pública” en procesos electorales¹⁸¹.

En **Paraguay**, la organización de derechos digitales TEDIC documentó la expansión de cámaras de reconocimiento facial instaladas desde 2018 por al menos 13 instituciones públicas sin marco legal que regule su uso a la fecha, sin estudios de impacto en derechos humanos y con fondos del Fondo de Servicio Universal desviados para financiar infraestructura de vigilancia¹⁸². En **Ecuador**, un decreto presidencial de septiembre de 2024 dispuso que el ECU-911 asumiera el control exclusivo de las cámaras de los gobiernos locales e implementara un sistema de videovigilancia en tiempo real con reconocimiento facial y de placas vehiculares¹⁸³.

Otra modalidad es el uso de plataformas de análisis masivo de datos. **Ecuador** formalizó una colaboración entre enero y mayo de 2025^{184 185} con Palantir Technologies para implementar su plataforma de análisis de datos en el Servicio Nacional de Aduana (SENAE), con el objetivo declarado de combatir el contrabando y fraude aduanero. Palantir es una empresa estadounidense cuya tecnología, desarrollada originalmente para operaciones de inteligencia del gobierno de Estados Unidos,

177. Mariana Milanes, et al., “Reconocimiento facial y tecnologías de vigilancia en América Latina: casos, proveedores y dinámicas comerciales”, *Al Sur* (Junio, 2025). Disponible en: <https://www.alsur.lat/sites/default/files/2025-07/Reporte%20reconocimiento%20facial.pdf>

178. Derechos Digitales, “Antes de cantar ‘Bad Romance’ te podrían estar vigilando”, [@derechos_digitales] (Mayo 2, 2025). Disponible en: https://www.instagram.com/derechos_digitales/p/DJKV6ARFF4/

179. Douglas Corrêa, “Seguridad reforzada para concierto de Lady Gaga en Copacabana”, *Agência Brasil* (Abril 29, 2025). Disponible en: <https://web.archive.org/web/20250430043836/https://agenciabrasil.ebc.com.br/es/cultura/noticia/2025-04/seguridad-reforzada-para-concierto-de-lady-gaga-en-copacabana>

180. ANRed, “Bullrich crea la Unidad de Inteligencia Artificial: ‘quiere hacer de la Argentina un Gran Hermano para espiarnos a todos’”, *ANRed* (Julio, 2024). Disponible en: <https://www.anred.org/bullrich-crea-la-unidad-de-inteligencia-artificial-quiere-hacer-de-la-argentina-un-gran-hermano-para-espiarnos-a-todos/>

181. Hugo Alconada Mon, “La SIDE pone la mira en quienes ‘manipulen la opinión pública’ o erosionen la confianza en los funcionarios”, *LA NACION* (Mayo 25, 2025). Disponible en: <https://www.lanacion.com.ar/politica/la-side-pone-la-mira-en-quienes-manipulen-la-opinion-publica-o-erosionen-la-confianza-en-los-nid25052025/>

182. TEDIC, “Con mi cara no: el Estado paraguayo despliega reconocimiento facial sin transparencia ni control”, *TEDIC* (Abril 29, 2025). Disponible en: https://www.tedic.org/comunicarano_estado/

183. Ecuavisa, “El ECU 911 accederá a los videos de las cámaras de seguridad de los GAD tras decreto presidencial”, *Ecuavisa* (Septiembre 18, 2024). Disponible en: <https://www.ecuavisa.com/ecuador/el-ecu-911-accedera-a-los-videos-de-las-cameras-de-seguridad-de-los-gad-tras-decreto-presidencial-20240918-0070.html>

184. Secretaría General de Comunicación de la Presidencia, “PALANTIR, ACTOR CLAVE EN SOFTWARE E INTELIGENCIA ARTIFICIAL PARA DEFENSA EN EE. UU., AHORA EN EL GOBIERNO DE NOBOA PARA COMBATIR DELITOS ADUANEROS”, *Gobierno del Ecuador* (Mayo 29, 2025). Disponible en: <https://www.comunicacion.gob.ec/palantir-actor-clave-en-software-e-inteligencia-artificial-para-defensa-en-ee-uu-ahora-en-el-gobierno-de-noboa-para-combatir-delitos-aduaneros/>

185. Redacción Ecuavisa, “El Gobierno anunció respaldo de Google, Palantir y Healthbird para la transformación digital de Ecuador”, *ECUAVISA* (Enero 23, 2025). Disponible en: <https://www.ecuavisa.com/politica/el-gobierno-anuncio-respaldo-de-google-palantir-y-healthbird-para-la-transformacion-digital-de-ecuador-20250123-0102.html>

permite el cruce masivo de datos de múltiples fuentes para identificar patrones y perfiles de personas en tiempo real. El contrato autoriza a SENAE a consolidar datos de otras entidades públicas en la plataforma de Palantir¹⁸⁶, lo que amplía el procesamiento de información más allá del control aduanero y por tanto, supone riesgos significativos para la privacidad de las personas y el control sobre sus propios datos.

Finalmente, otra dimensión de vigilancia digital documentada en la región es el monitoreo del discurso en redes sociales. Derechos Digitales documentó dos prácticas desplegadas por gobiernos de la región¹⁸⁷: el perfilamiento, que consiste en caracterizar a personas usuarias de redes sociales según si sus publicaciones son favorables, críticas u opositoras al gobierno; y el ciberpatrullaje, que implica el monitoreo encubierto de la actividad en línea con el fin de identificar y perseguir penalmente a personas por sus actividades en internet. Ambas operan bajo la premisa de que cualquier contenido publicado en internet es de libre uso por parte del Estado, incluso con fines de persecución, lo que organizaciones de derechos humanos han cuestionado¹⁸⁸.

En **Colombia**, una investigación reveló que el gobierno contrató a una empresa para posicionar favorablemente su imagen ante la opinión pública; en la práctica, ello derivó a la elaboración de un listado de 486 personas usuarias de X clasificadas según su posición favorable, neutral u opositora al gobierno. En **Brasil**, en 2024 se conoció una licitación del gobierno federal para contratar servicios de perfilamiento en redes sociales, justificada como una herramienta para medir popularidad del gobierno, analizar emociones de personas usuarias mediante IA y combatir la desinformación¹⁸⁹.

En **México**, una investigación de 2024 basada en documentos filtrados por el colectivo Guacamaya reveló que la Secretaría de Defensa adquirió en 2020 el software israelí HIWIRE para monitorear en tiempo real a personas usuarias críticas del ejército, mapear sus interacciones y crear cuentas falsas para interactuar de forma encubierta con los objetivos¹⁹⁰.

El ciberpatrullaje como práctica se ha extendido por la región con distintos niveles de regulación y opacidad: en **Uruguay**, la Dirección General de la Policía reconoció en 2024 que monitoreaba redes sociales. Ese mismo año, un adolescente fue detenido tras ser identificado erróneamente como participante de enfrentamientos en centros educativos, al ser confundido con un homónimo en redes sociales¹⁹¹.

186. Ibid

187. Lucía Camacho, "Perfilamiento en redes sociales y ciberpatrullaje como nuevas modalidades de la vigilancia masiva desplegada por los Estados: casos relevantes en América Latina", Derechos Digitales (Agosto, 2024). Disponible en: https://www.derechosdigitales.org/wp-content/uploads/Informe-RELE-vigilancia-masiva_cerrado.pdf

188. Ximena Cuzcano, "Ciberpatrullaje: cuando vigilar se justifica en nombre de la seguridad", Derechos Digitales (Mayo 9, 2025). Disponible en: <https://www.derechosdigitales.org/recursos/ciberpatrullaje-cuando-vigilar-se-justifica-en-nombre-de-la-seguridad/>

189. Lucía Camacho, Perfilamiento en redes sociales y ciberpatrullaje como nuevas modalidades de la vigilancia masiva desplegada por los Estados: casos relevantes en América Latina", Derechos Digitales (Agosto, 2024). Disponible en: https://www.derechosdigitales.org/wp-content/uploads/Informe-RELE-vigilancia-masiva_cerrado.pdf

190. Ibid

191. Ibid

En otros países, el ciberpatrullaje ha sido incorporado o reinstaurado en marcos normativos: en **Argentina** fue reinstaurado en la normativa local en 2024 tras haber sido derogado en 2022; y en **Paraguay** fue incorporado a la ley de reforma y modernización de la Policía Nacional en junio de 2024¹⁹².

192. Ibid

5. Conclusiones



5 Conclusiones

En la mira 2 busca llenar un vacío en la documentación regional sobre incidentes de seguridad digital y prácticas de vigilancia analizada de manera sistematizada y desde una perspectiva de derechos humanos e interés público. La información existe y es valiosa; sin embargo, esta se encuentra dispersa en múltiples fuentes sin un espacio que las integre y le dé sentido a nivel regional. Por ello, el valor de este ejercicio no está en ofrecer un ranking de países, sino en reunir, ordenar y dar sentido a casos que, vistos de forma aislada, podrían parecer inconexos, pero que en conjunto permiten identificar actores, tecnologías, tendencias regionales de afectación, y rastrear trayectorias en el tiempo.

En ese sentido, los casos documentados no deben leerse como una muestra representativa ni como una comparación directa entre países. La mayor o menor presencia de incidentes en un país puede responder a múltiples factores como la capacidad de monitoreo de organizaciones locales, coyunturas específicas del período, o cambios de gobierno que alteran drásticamente el panorama de un año a otro. Comparar números entre países sin considerar estas variables puede llevar a conclusiones equivocadas.

La vigilancia, la persecución a periodistas y activistas, y el cierre del espacio cívico dificultan directamente el trabajo de las organizaciones que monitorean estos fenómenos, tal como ocurre en **Nicaragua**, donde más de 2.600 organizaciones de la sociedad civil fueron disueltas entre 2018 y 2022¹⁹³. Pero incluso en países con instituciones más consolidadas, como **Argentina** y **México**, se observa una tendencia creciente a restringir el acceso a la información, lo que representa una preocupación regional que trasciende las clasificaciones habituales entre democracias y autoritarismos.

193. Mayra Osorio, "Derechos humanos en entornos digitales en Nicaragua", Derechos Digitales (Octubre 11, 2023). Disponible en: <https://www.derechosdigitales.org/recursos/derechos-humanos-en-entornos-digitales-en-nicaragua/>

Aun con esas limitaciones, el informe demuestra que los incidentes de seguridad digital no pueden analizarse como hechos puramente técnicos; los casos documentados responden a contextos políticos específicos. Por ello, iniciativas de seguridad digital que no toman en cuenta ese contexto corren el riesgo de ofrecer respuestas parciales: proteger un dispositivo no protege de manera íntegra a una persona cuya organización está siendo perseguida por el Estado, ni a una periodista cuyo medio fue clausurado. Comprender esa dimensión es indispensable para que las respuestas en materia de seguridad digital sean verdaderamente efectivas.

El informe también evidencia una tensión preocupante entre la rápida adopción o legitimación de tecnologías y prácticas de control, y la lentitud con que avanzan los mecanismos de transparencia y protección de derechos. En particular, se observan intentos de validar legalmente prácticas como el ciberpatrullaje o ampliar capacidades estatales de análisis y vigilancia, sin que ello venga acompañado, en igual medida, de mecanismos proporcionales de control y rendición de cuentas.

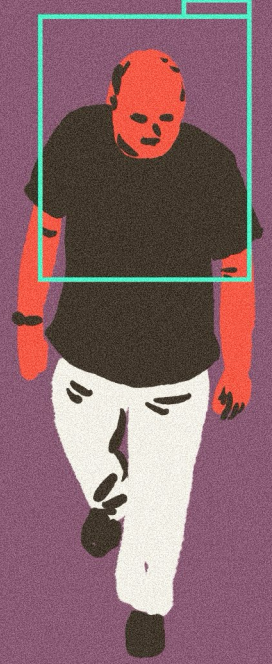
Un elemento que distingue este informe de su edición anterior es la presencia creciente de la IA como vector transversal en los incidentes documentados. Su aparición en múltiples secciones, refleja el desafío de comprender la IA no solo como herramienta de innovación, sino como parte de infraestructuras más amplias de poder, clasificación, control y producción de daño, cuyos efectos no recaen de manera uniforme sobre todas las personas. Un ejemplo claro es la generación de *deepfakes* sexualizados, que se ha convertido en una práctica de violencia y control dirigido de forma particular contra las mujeres. Sin embargo, cabe resaltar que el surgimiento de estas nuevas tecnologías no reemplaza formas más tradicionales de represión y control. En Centroamérica, por ejemplo, se observa la persistencia de múltiples mecanismos que combinan herramientas tecnológicas, reformas legales restrictivas y persecución política, operando de manera simultánea y reforzándose mutuamente.

A lo largo de este informe se hace visible que los impactos de los incidentes no se distribuyen de manera homogénea. Periodistas, activistas, opositores políticos, mujeres, personas LGBTIQ+, comunidades migrantes, poblaciones empobrecidas o personas con menor acceso a recursos digitales enfrentan riesgos específicos según el tipo de tecnología o ataque. En varios casos, la afectación trasciende lo individual y produce efectos colectivos, como autocensura, inhibición de la protesta, debilitamiento de redes de apoyo o reducción del espacio cívico.

Esta distribución desigual de los impactos puede atribuirse tanto a actores estatales como privados. Por ejemplo, los primeros utilizan software de vigilancia para perseguir a opositores políticos. Mientras que en el ámbito privado destacan casos como el de World, que compra masivamente datos biométricos, o el de las aplicaciones de préstamos que implementan mecanismos de extorsión; dos casos que ilustran cómo la tecnología se emplea para aprovecharse de las condiciones económicas de la población.

Finalmente, cabe señalar que la eliminación de fondos por parte del gobierno de Estados Unidos y el cierre de USAID en 2025¹⁹⁴ tuvieron un fuerte impacto en las organizaciones de la sociedad civil de la región. Esta situación dificultó la articulación del trabajo del OLAD y retrasó la publicación del presente informe. No obstante, el apoyo sostenido de sus miembros fue fundamental para que este informe pudiera concretarse por lo que queremos agradecerles por su colaboración en el desarrollo de En la mira 2.

194. Débora Calderón, "Recalculando: nuevas estrategias para enfrentar los ajustes en la cooperación internacional", Derechos Digitales (Julio 11, 2025). Disponible en: <https://www.derechosdigitales.org/recursos/recalculando-nuevas-estrategias-para-enfrentar-los-ajustes-en-la-cooperacion-internacional/>



 Derechos
Digitales
AMÉRICA LATINA

