

The background of the entire page is a dark purple. Overlaid on this are stylized, high-contrast illustrations of various people in different poses and outfits. Each person is enclosed within a thin, light blue rectangular border, which is slightly offset from the top-left corner of the person's figure, 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 dress and black shoes, a man in a black t-shirt and black shorts, a woman in a white shirt and black pants, a man in a white t-shirt and black pants with a backpack, and a woman in a white shirt and black pants. The overall aesthetic is modern and digital.

In Focus 2: An overview of digital threats in Latin America

In Focus 2:

An overview of digital threats in Latin America

This publication was produced by Derechos Digitales, an independent non-profit organization founded in 2005, whose mission is the defense, promotion, and development of fundamental rights in digital environments in Latin America.

General supervision: Rafael Bonifaz

Coordination and review: Rafael Bonifaz and Jamila Venturini

Analysis and writing: Ximena Cuzcano

Research: Ximena Cuzcano

Revision and Proofreading: Gastón Wahnish

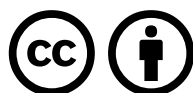
Design: Diego Lepián

This report is the result of a joint work within the Latin American Observatory on Digital Threats (OLAD), an alliance of Latin American organizations that include Código Sur (regional), Colnodo (Colombia), Conexión Segura (Venezuela), Derechos Digitales (regional), Escola de Ativismo (Brazil), Fundación Acceso (regional), Fundación InternetBolivia.org (Bolivia), Fundación Karisma (Colombia), Instituto Nupef (Brazil), LaLibre.net Tecnologías Comunitarias (Ecuador), MariaLab (Brazil), Social TIC (Mexico), Sursiendo (Mexico) and Taller de Comunicación Mujer (Ecuador).

August, 2026

How to cite this publication: Derechos Digitales. (2026). In Focus 2: An overview of digital threats in Latin America.

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



This work is licensed under Creative Commons Attribution 4.0 International.

<https://creativecommons.org/licenses/by/4.0/deed.es>

Index

1 Introduction	4
2 Methodology	7
3 The digital security landscape in Latin America	10
3.1. Regulatory framework	11
3.2. Censorship	14
3.3. Data breaches	17
3.4. Disinformation during elections	22
3.5. Targeted attacks	24
4 Thematic areas	28
4.1. Technology-Facilitated Gender-Based Violence	29
4.1.1. Navegando Libres	30
4.1.2. S.O.S. Digital	31
4.1.3. Other cases	32
4.2. Exploitation of biometric data	33
4.3. Internet shutdowns	37
4.4. Surveillance	39
5 Conclusions	46



1. Introduction

1 Introduction

Internet and digital technologies are central spaces for the exercise of human rights in Latin America. Through them, communities access essential information and services, activists organize and coordinate, and journalists document abuses of power and keep the public informed. Keeping this space free and safe is a necessary condition for exercising fundamental rights. However, this same space has also become a setting for surveillance, censorship, violence, and control. Unlike cybersecurity reports that focus on economic and commercial impacts, this report aims to shed light on how digital threats and attacks affect the work of civil society and the exercise of fundamental rights across the region.

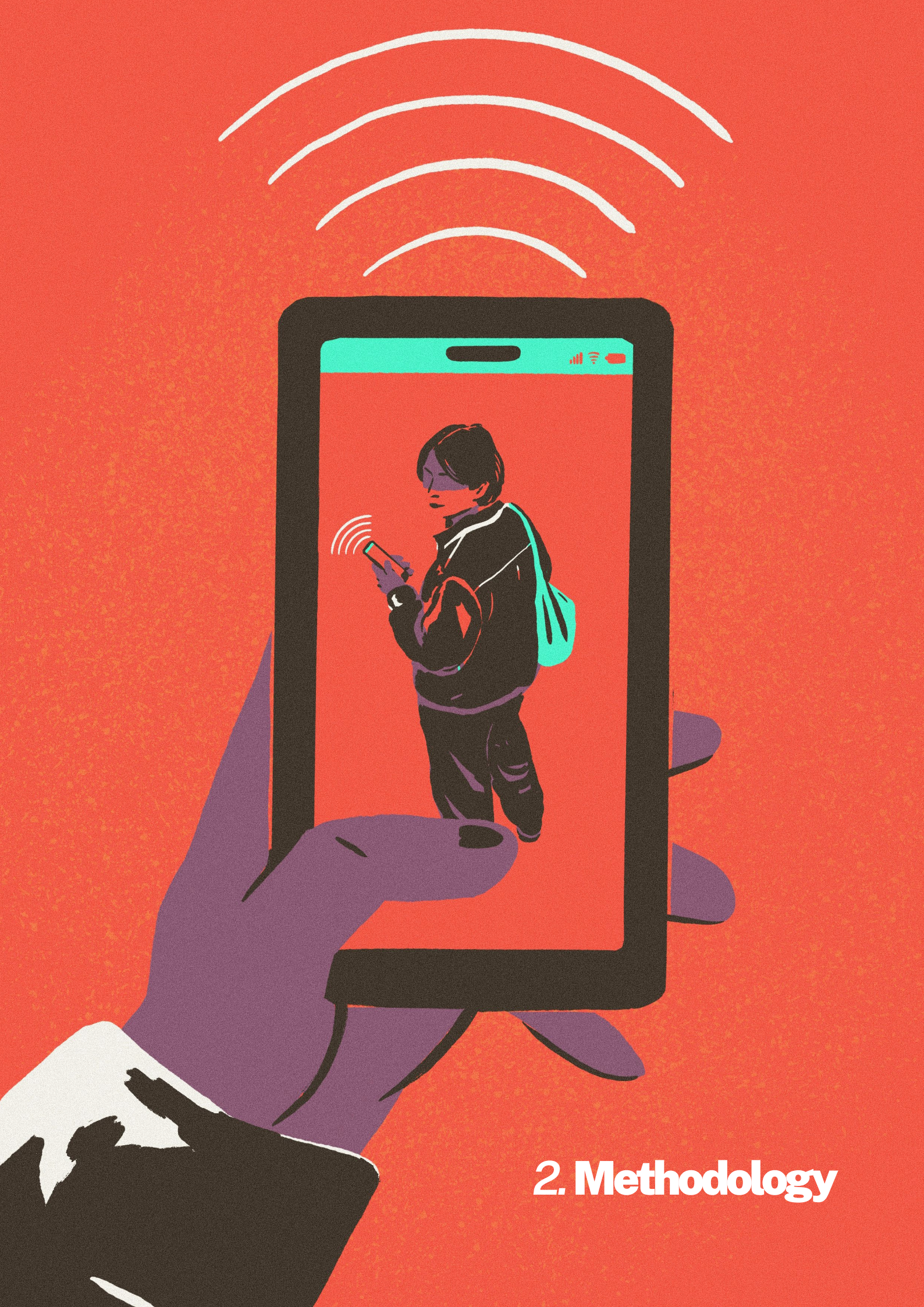
In Focus 2: An overview of digital threats in Latin America is the result of work led by Derechos Digitales as part of the Latin American Observatory on Digital Threats (OLAD), an alliance of Latin American organizations dedicated to defending human rights in the digital sphere. The Observatory facilitates the exchange of knowledge and experiences related to digital security and serves as a platform for monitoring incidents from a human rights and public interest perspective.

The following organizations are part of this alliance: Código Sur (regional), Colnodo (Colombia), Conexión Segura (Venezuela), Derechos Digitales (regional), Escola de Ativismo (Brazil), Fundación Acceso (regional), Fundación InternetBolivia.org (Bolivia), Fundación Karisma (Colombia), Instituto Nupef (Brazil), LaLibre.net Tecnologías Comunitarias (Ecuador), MariaLab (Brazil), Social TIC (Mexico), Sursiendo (Mexico), and Taller de Comunicación Mujer (Ecuador). This second installment draws particularly on reports and research produced by several of these organizations.

Each OLAD member organization fulfills different functions depending on its country context and area of expertise. Working across different territories and fields, they produce knowledge, support cases, investigate threats, and raise awareness about practices that affect online rights. Based on the work of these organizations and through regular monitoring, Derechos Digitales has led the drafting of this report to shed light on how digital threats affect the exercise of rights in Latin America.

In Focus 2 builds on the work of the first report in this series. We understand that the documentation accumulated over time is, in itself, a tool for advocacy and memory. It also constitutes an essential mechanism for future accountability, since in authoritarian contexts where there are currently no conditions to investigate, sanction, or remedy violations, preserving evidence and maintaining rigorous records makes it possible to uphold the truth of the facts, strengthen justice processes—for when conditions change—and even reduce the risk that these abuses will go unpunished.

The report is organized into two main sections. The first, *Digital security context in Latin America*, provides a regional overview through five key areas: regulatory developments during the period, censorship in digital environments, data breaches, disinformation in electoral processes, and targeted attacks. The second section, *Thematic areas*, examines four trends in digital incidents during this period: surveillance, the exploitation of biometric data, internet shutdowns, and technology-facilitated gender-based violence.



2. Methodology

2 Methodology

The *In Focus 2* report presents a regional overview of digital security incidents that affect the exercise of human rights in Latin America. The analysis covers the period from June 2024 to May 2025. For the purposes of this report, incidents are defined as events related to the use, control, or abuse of digital technologies that have impacts on rights such as freedom of expression, privacy and data protection, access to information, the integrity and security of individuals and groups, as well as civic participation in digital environments.

The information analyzed was collected through two complementary channels. First, a systematic weekly monitoring of open sources was conducted, focusing primarily on news published by media outlets, reports available online, and publicly reported data breach incidents. This approach makes it possible to identify regional trends and document incidents that receive public attention; however, it has significant limitations. Media coverage varies across countries, many incidents are never reported, and in contexts of censorship or a weak press, a significant share of events remains outside the public record.

Second, the report incorporates information and insights from the organizations that make up OLAD, which work directly to support individuals and organizations affected by digital attacks, as well as to investigate and/or monitor such incidents across the region. This collaboration helps fill gaps in news monitoring and shed light on dynamics that are not always visible in open-source information. However, this approach also has limitations, as not all cases can be publicly disclosed without increasing risks for those affected or for those supporting these processes. Consequently, the report's findings should not be interpreted as a ranking of incidents or as a comparative assessment across countries, but rather as a context-specific analysis of regional patterns and dynamics.

During the period analyzed, these limitations have been exacerbated by an increasingly hostile global environment for civil society. Various organizations face restrictions on civic space, increased surveillance and stigmatization of their work, as well as challenges to their financial sustainability, amid cuts or freezes in international funding for human rights and technology initiatives. These conditions directly affect their ability to continuously monitor and document cases and must be taken into account when interpreting the report's findings.

Finally, the information collected was organized into thematic areas that allow for the analysis of patterns and types of incidents at the regional level. In all cases, a reasonable verification standard was applied, prioritizing source traceability and avoiding conclusions that could not be supported by publicly available evidence. Furthermore, the report adopts a do-no-harm approach, taking care not to publish details that could lead to revictimization or pose additional risks to affected individuals and communities.



3. The digital security landscape in Latin America

3

The digital security landscape in Latin America

This chapter provides an overview of the digital security landscape in Latin America during the period under review, based on systematizing and analyzing open-source monitoring. Rather than presenting an exhaustive inventory of incidents, it seeks to contextualize the main phenomena observed in the region and understand how they manifest across the board, distinguishing impacts on different countries and social groups.

3.1. Regulatory Framework

Regional monitoring identified relevant regulatory developments across several Latin American countries that directly affect the exercise of human rights in the digital environment. Legislative and regulatory initiatives related to state surveillance, restrictions on freedom of expression—including censorship mechanisms—and restrictions on access to public information emerged repeatedly. These themes reflect state responses that shape the political and legal context enabling—and in some cases legitimizing—the digital security incidents analyzed in the following sections.

The regulatory developments described reflect the status of each legislative or regulatory process as of the end of the period under review. Given the dynamic nature of these processes, some initiatives may have progressed, been amended, or been shelved since then. Their evolution will therefore remain part of the ongoing monitoring that underpins this report.

A first observable regulatory trend is the expansion of legal frameworks that **broaden state surveillance powers** in digital environments, generally justified on the grounds of national security and public order. In **Argentina**, Resolution

428/2024 of the Ministry of Security formalized a crime-prevention protocol that authorizes systematic monitoring of open sources and the use of automated technologies to analyze online information¹. As of the end of the reporting period, Decree 383/2025 had explicitly established cyber-patrolling as a power of this law enforcement agency, without requiring judicial authorization when dealing with open sources² ³. In **Paraguay**, Law 7269/2024 introduced mandatory biometric surveillance using facial recognition systems in soccer stadiums, extending mass surveillance practices to public spaces⁴. In **Mexico**, various initiatives to amend the National Security Law ambiguously broadened the definition of security threats, paving the way for expanded state surveillance powers and information control⁵. In **Ecuador**, the approval of a new Intelligence Law created a National Intelligence System with broad powers to intercept communications and access telecommunications data without a court order⁶. As of the end of the reporting period, the Constitutional Court was reviewing the law after constitutional challenges questioned whether these powers were compatible with fundamental rights. However, the Executive Branch had already issued implementing regulations authorizing intelligence agencies to request information from telecommunications providers on geolocation, data traffic, and call records without a court order⁷. In **Venezuela**, the National Cybersecurity Council was created by decree, consolidating a state-led cyber-surveillance approach with extensive powers, framed around narratives of cyber threats associated with social media and opposition actors⁸.

In contrast, **Colombia** introduced Statutory Bill 225 to amend Law 1621 of 2013, aiming to strengthen human rights protections and reinforce the legal framework governing agencies that carry out intelligence and counterintelligence activities, in compliance with a ruling by the Inter-American Court of Human Rights⁹. The bill received a favorable report for its first debate in November 2024, but was not debated before the end of the legislative session and was therefore shelved¹⁰.

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

2. República Argentina, “Decreto 383/2025”, *Boletín Oficial de la República Argentina* (June 16, 2025). Available at: <https://www.boletinoficial.gob.ar/detalleAviso/primera/326993>

3. Rosario Marina, “Ciberpatrullaje: qué dice el nuevo decreto y qué implican los cambios en la Policía Federal”, *Chequeado* (June 18, 2025). Available at: <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 (December 12, 2024). Available at: <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 (October 14, 2024). Available at: <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* (June 23, 2025). Available at: <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* (July 14, 2025). Available at: <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* (August 21, 2024). Available at: <https://elestimulo.com/venezuela/2024-08-21/consejo-nacional-de-ciberseguridad/>

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* (October 1, 2024). Available at: <https://www.comisionprimerasenado.com/documentos-pendientes-de-publicacion/ponencias-y-textos-aprobados/4148-ponencia-ple-225-de-2024-inteligencia-y-contrainteligencia/file>

10. Under Article 153 of the Political Constitution of Colombia, statutory laws must be processed and approved within a single legislative session.

Another relevant regulatory development directly affects **freedom of expression and the implementation of digital censorship mechanisms**. In El Salvador, the passage of the Cybersecurity Law and the creation of the State Cybersecurity Agency (ACE) consolidated a highly centralized institutional framework with regulatory, oversight, and enforcement powers that could facilitate removing online content¹¹. In **Colombia**, Bill 023 of 2023, debated in 2024, proposes the creation of a Digital Security Agency with exceptional powers to order the cessation of operations in cyberspace, meaning the temporary interruption of platforms or digital services in situations defined as crises. Its implementation could entail suspending social media or digital media outlets, thereby affecting the circulation of information¹². In **Cuba**, the Social Communication Law, in force since 2024, establishes a comprehensive regulatory framework for digital content and media that reinforces state control over the production and circulation of information, particularly affecting independent media and non-state forms of expression¹³. In **Nicaragua**, amendments to Law 1042, the Special Cybercrime Law, expanded the range of conduct subject to criminalization related to the dissemination of information online and established a framework used to penalize digital expression and create a chilling effect on journalism, activism, and civil society¹⁴.

Similarly, legal reforms have weakened institutional mechanisms for **access to public information**, undermining transparency and accountability. In **Mexico**, constitutional amendments passed between 2024 and 2025 eliminated the National Institute for Transparency, Access to Information and Protection of Personal Data (INAI) as an autonomous body¹⁵. This limits citizens' ability to understand and monitor government actions and to participate in public affairs in an informed manner. In **Argentina**, the 2024 amendments to the public information access regime expanded the grounds for withholding information and narrowed what counts as public information¹⁶. This reform reduces the government's obligation to disclose information of public interest and weakens citizens' ability to hold it accountable.

In parallel, regulatory tensions persist around **personal data protection**, where regulatory advances coexist with legal frameworks that enable surveillance practices. In **Chile**, the passage of Law 21,719 on Personal Data Protection and Law 21,663, the Cybersecurity Framework Law, strengthened the institutional

11. Human Rights Watch, "El Salvador: New Laws Threaten Free Expression, Privacy", Human Rights Watch (December 12, 2024). Available at: <https://www.hrw.org/news/2024/12/12/el-salvador-new-laws-threaten-free-expression-privacy>

12. Mateo García Agudelo, "¿Gobierno del presidente Petro busca, con proyecto de ley, facultades para apagar las redes sociales en Colombia?", El Tiempo (September 25, 2024). Available at: <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 (June 6, 2024). Available at: <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 (October 8, 2024). Available at: <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 (December 11, 2024). Available at: <https://r3d.mx/2024/12/11/requiem-por-el-inai-un-retroceso-para-la-defensa-de-los-derechos-digitales/>

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

framework in this area and expanded rights¹⁷. However, these advances coexist with provisions authorizing the use of surveillance technologies, such as communications interception devices (IMSI catchers), under anti-terrorism legislation¹⁸. In **El Salvador**, the Personal Data Protection Act was implemented alongside a cybersecurity framework in which national security and public order objectives are defined broadly and vaguely, with limited institutional safeguards¹⁹. This raises questions about how effectively individuals' rights are prioritized over security objectives.

3.2. Censorship

The censorship landscape in digital environments across Latin America between June 2024 and May 2025 reveals an increasingly adaptable and technically complex ecosystem of control. Governments have combined infrastructure-blocking techniques with pressure on private actors and legal persecution to stifle online freedom of expression. These measures are not isolated; rather, they tend to intensify strategically during critical moments such as elections or social protests, combining technical tools with institutional or coercive mechanisms. They also hit journalists, activists, and people with fewer technical resources harder, widening digital divides and gaps in access to information.

The following describes the main incidents observed in this regard, organized by country.

Regarding **platform and social media blocking**, following the 2024 elections, the Venezuelan government, through orders issued by the National Telecommunications Commission (CONATEL) to internet service providers, carried out a massive wave of blocks affecting platforms such as Signal, X, TikTok, Telegram, and YouTube^{20 21 22 23}. Even corporate services such as Microsoft Teams, statistical websites such as Statista, and entertainment platforms such as Disney+, Max, and Amazon Prime Video were blocked²⁴. Censorship reached a particularly critical level, ac-

17. Juan Carlos Lara, "Los desafíos de la nueva Ley de Protección de Datos Personales", CIPER Chile (January 28, 2025). Available at: <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 (December 11, 2024). Available at: <https://www.latercera.com/politica/noticia/en-medio-de-ten-sa-sesion-congreso-aprueba-ley-antiterrorista/BY2SGOUJONH5JHEGFBSLC5LZR4/>

19. Human Rights Watch, "El Salvador: New Laws Threaten Free Expression, Privacy", Human Rights Watch (December 12, 2024). Available at: <https://www.hrw.org/news/2024/12/12/el-salvador-new-laws-threaten-free-expression-privacy>

20. Regina Garcia Cano, "Maduro suspends X social network in Venezuela for 10 days", AP News (August 9, 2024). Disponible: <https://apnews.com/article/venezuela-elections-suspension-x-elon-musk-59bb734bdd0c8cc4082d6a0c-b0f5af25>

21. Sergio Henostroza, "Usuarios reportan bloqueo masivo de TikTok en Venezuela y responsabilizan al régimen de Nicolás Maduro", La República (September 29, 2024). Available at: <https://larepublica.pe/mundo/venezuela/2024/09/28/usuarios-reportan-bloqueo-masivo-de-tiktok-en-venezuela-y-responsabilizan-al-regimen-de-nicolas-maduro-lrt-mc-613984>

22. Jay Peters, "Signal Has Been Blocked by Venezuela and Russia", The Verge (August 9, 2024). Available at: <https://www.theverge.com/2024/8/9/24217008/signal-blocked-venezuela-russia>

23. VE sin Filtro, "Bloquean nuevamente Telegram en Venezuela", [@vesinfiltro] (May 2, 2025). Available at: <https://x.com/vesinfiltro/status/1918276217746174061>

24. In practice, these blocks are typically implemented through technical interference, often at the DNS level (in domain name resolution), to prevent access without cutting off the entire Internet connection.

cording to the VE Sin Filtro²⁵ report: between July 2024 and January 2025, 79 new website blocks were documented, in addition to 89 existing ones, many of which targeted independent media outlets. In addition, websites of VPN providers²⁶ such as Proton and Windscribe were blocked to prevent people from circumventing the imposed restrictions and to protect their online privacy.

Furthermore, the state-owned internet service provider (ISP) CANTV blocked more than 30 public DNS servers, including those operated by Google and Cloudflare²⁷. DNS functions as the internet's "phone book": it translates domain names (for example, a website's address) into IP addresses that allow users to access content. In practice, most people use the DNS provided by their internet service provider, such as CANTV. This lets the provider restrict access to certain sites by blocking or manipulating DNS resolution. In these situations, a common workaround is to switch DNS providers to try to regain access.

There were also instances of censorship aimed at disrupting media availability. In August 2024, the website of the newspaper TalCual was targeted by a distributed denial-of-service (DDoS) attack. This technique floods a server with massive amounts of traffic from multiple locations, rendering it inaccessible. The attack disrupted access for approximately four hours²⁸.

In **Brazil**, the Supreme Federal Court ordered the complete suspension of X after the platform repeatedly failed to comply with court orders to appoint a legal representative in the country and remove accounts linked to disinformation. The decision also imposed penalties on those who attempted to circumvent the suspension using a VPN. While the suspension has a legal basis in the Brazilian Civil Rights Framework for the Internet, its broad scope affected all users of the platform in the country, raising questions about its proportionality under Inter-American standards on freedom of expression²⁹.

In **Colombia**, the state agency Coljuegos—which regulates games of chance—ordered internet service providers to block Reddit on the grounds that the domain was linked to unauthorized gambling operators, under the authority granted by Law 1753 of 2015³⁰. The block was implemented through DNS redirects and restrictions, a measure confirmed by independent tests conducted using the OONI

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

26. A Virtual Private Network (VPN) is a tool that encrypts your internet connection and reroutes traffic through servers in other countries, allowing you to browse privately and bypass geographic blocks or restrictions imposed by internet service providers.

27. Redacción Voz de América, "Venezuela muestra 'cifras alarmantes' de censura digital, denuncia Ve Sin Filtro", Voz de América (March 14, 2025). Available at: <https://www.vozdeamerica.com/a/venezuela-cifras-alarmanentes-censura-digital/8010029.html>

28. IPYS Venezuela, "Sitio web del diario TalCual fue objeto de un ataque DDoS", Voces del Sur (August 12, 2024). Available at: <https://vocesdelsurunidas.org/incidentes/sitio-web-del-diario-talcual-fue-objeto-de-un-ataque-ddos/>

29. Lucía Camacho, "La suspensión de X en Brasil, y la vigencia del Estado de Derecho", Derechos Digitales (September 11, 2024). Available at: <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 (June 7, 2024). Available at: <https://blog.karisma.org.co/las-dudas-que-quedan-tras-el-bloqueo-de-reddit-en-colombia/>

tool³¹. Although the measure was temporary, it raised questions about its proportionality and the lack of clarity regarding the criteria used to include websites on official blocking lists³².

Regarding **attacks and interference targeting Internet infrastructure and Domain Name System (DNS) infrastructure**, in **Nicaragua**, the National University of Engineering (UNI), the state institution that administers the national .ni domain through NIC.NI, arbitrarily blocked the domains of independent media outlets such as Confidencial, La Prensa, Onda Local, and 100% Noticias, without a documented order or notification, forcing them to migrate to international domains to continue operating³³.

A similar attempt occurred in the **Dominican Republic**, when the U.S. company Network Solutions issued an ultimatum to the newspaper Listín Diario, demanding that it remove a report on corruption under threat of suspending its web hosting³⁴. The company cited an alleged violation of its terms of service after receiving a takedown request³⁵. This case highlights the role private companies at the infrastructure level can play in imposing indirect censorship by using vague contractual clauses to suppress information of public interest.

In **Cuba**, the government uses Deep Packet Inspection (DPI)³⁶ technology to analyze traffic in real time and block encrypted messaging apps such as Signal and DeltaChat³⁷. In addition, the state-owned telecommunications company ETEC-SA deliberately imposes complete internet shutdowns during social protests and raises rates to limit public access³⁸.

Also in **Cuba**, in August 2024, a person was sentenced to one and a half years in prison after posting a meme featuring images of government officials, while at least four others were detained and questioned over social media posts³⁹. Between September and October, the wave of repression led to the closure of at least one media outlet, the questioning and threat of imprisonment of four media directors,

31. OONI is a project and suite of open-source software tools developed by The Tor Project, whose goal is to monitor, measure, and document internet censorship, traffic manipulation, and interference in telecommunications networks worldwide. Available at: <https://ooni.org>

32. Lucía Camacho, “La suspensión de X en Brasil, y la vigencia del Estado de Derecho”, *Derechos Digitales* (September 11, 2024). Available at: <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* (March 14, 2025). Available at: <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* (May 15, 2025). Available at: <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* (May 15, 2025). Available at: https://listindiario.com/la-republica/20250515/comunicado-listin-diario-censura-digital_857815.html

36. Deep Packet Inspection (DPI) is a network traffic analysis technology that, unlike conventional filtering methods, allows for the examination of the full content of data packets traveling over the Internet, rather than just their source or destination. This enables the network administrator to selectively identify and block specific applications, protocols, or content, even when encryption tools are used.

37. Diktyon, “Informe #6 sobre la salud del Internet en Cuba”, *Guardianes Digitales* (October, 2024). Available at: <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* (June 1, 2025). Available at: <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 (August de 2024)”, *Yucabyte* (September, 2024). Available at: <https://www.yucabyte.org/2024/09/26/violaciones-de-derechos-digitales-en-cuba-agosto-de-2024/>

and the resignation of at least nine journalists and activists^{40 41}.

Cases of judicial persecution were documented in **Honduras**, where news outlet Hondudiario was investigated for “publicly disseminated insult” after reporting on internal tensions within the Armed Forces in a post on X⁴². In **El Salvador**, the Attorney General’s Office prepared arrest warrants for journalists from El Faro following an investigation published on YouTube into government deals with gangs⁴³.

3.3. Data Breaches

Governments and companies store large volumes of personal data to operate services, administer programs, and manage day-to-day transactions. When data is processed without adequate security and governance standards or through poorly controlled outsourcing arrangements, the risk of exposure or unauthorized access increases. In this context, personal data breaches have become one of the most common occurrences in the region’s digital security landscape.

A data breach occurs when unauthorized individuals access personal or confidential information stored by public or private entities. This can enable fraud, extortion, surveillance, or violence. Unlike other types of incidents associated with specific circumstances, data breaches stem from poor organizational practices that recur across countries and sectors, such as excessive data collection, outsourcing technology without adequate controls, and weak mechanisms for protecting and monitoring access, in a context where several countries in the region still lack regulatory frameworks for personal data protection. This report identifies specific cases in 12 countries⁴⁴, as well as data breaches with regional reach.

One of the most common types of data breaches identified was not the result of sophisticated cyberattacks, but rather of basic data protection errors. In particular, multiple incidents resulted from **misconfigurations** that left databases accessible without authentication. Put simply, this is like leaving confidential files in a public space without a lock. In Colombia, the GoPass payment app left a Google Cloud Storage⁴⁵ bucket open, exposing the data of nearly one million people, including vehicle registration numbers and tax identification numbers⁴⁶.

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

41. Yucabyte, “Violaciones de derechos digitales en Cuba (October 2024)”, YucaByte (November 27, 2024). Available at: <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 «Hondudiario» por supuesto delito de injuria”, ARTICLE 19 (February 2, 2025). Available at: <https://articulo19.org/unidad-contra-delitos-informaticos-de-la-interpol-de-honduras-investiga-a-medio-hondudiario-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 (May 9, 2025). Available at: <https://www.fidh.org/es/region/americas/el-salvador/el-salvador-escalada-de-persecucion-y-ataques-a-la-libertad-de-prensa>

44. Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, Honduras, Mexico, Paraguay, Peru, Uruguay, and Venezuela.

45. Google Cloud Storage: Google’s cloud storage service that allows you to store and access large volumes of data using containers called buckets. Incorrect permission settings can cause these buckets to become public and expose sensitive information without authentication.

46. Paulina Okunyté, “Cashless Toll Payments End with Massive Data Leak”, Cybernews (September 19, 2024). Available at: <https://cybernews.com/security/gopass-colombia-data-leak/>

In **Costa Rica**, a misconfiguration in Movistar's infrastructure left nearly 650,000 files containing identification documents, work permits, and selfies used in identity verification processes accessible⁴⁷. **At the regional level**, the digital banking platform Bankingly exposed the personal and financial data of more than 135,000 customers of cooperatives and microfinance institutions in countries including Bolivia, Costa Rica, Ecuador, El Salvador, Mexico, and the Dominican Republic after using Azure⁴⁸ storage containers without adequate security measures⁴⁹.

Another significant set of incidents involved **digital supply chain vulnerabilities**, where data breaches occur not directly within the main organization but at technology providers with access to its systems. In **Peru**, the leak of Interbank's customer data stemmed from misused credentials that allowed access to servers managed by an external monitoring provider, highlighting critical risks from outsourcing⁵⁰.

A similar pattern emerged in **Argentina**, where attackers compromised an SMS messaging service provider responsible for sending one-time passwords (OTPs) and messages related to authentication and account recovery⁵¹. After compromising this SMS messaging gateway, attackers were able to intercept SMS traffic in real time, including OTPs. This facilitated account takeovers through password reset processes and other flows that rely on SMS verification, reducing the effectiveness of two-factor authentication when it relies on text messages.

Regional monitoring also identified data breaches resulting from the **abusive use of legitimate**, formally authorized access credentials; however, it could not be determined whether the actions were carried out by the account holders themselves or by third parties who had gained access to those accounts. In Peru, the exposure of images and personal data stored in RENIEC's⁵² databases was attributed to the misuse of access credentials assigned to the Ministry of the Interior⁵³.

Similarly, an investigation was launched in **Ecuador** into a data leak from the ECU 911 emergency service to funeral service companies. This allowed the companies to contact relatives of people in critical condition even before a death occurred, raising ethical and data protection concerns in contexts of vulnerability⁵⁴.

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

48. Azure Containers: Microsoft cloud storage spaces used to store and manage files and data. If configured incorrectly, they can allow unauthorized access to sensitive information.

49. El Testigo, "Una filtración de datos afecta a las instituciones financieras de América Latina, incluida República Dominicana", El Testigo (December 4, 2024). Available at: <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 (November 10, 2024). Available at: <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 (March 30, 2025). Available at: https://www.clarin.com/tecnologia/hackean-proveedor-mensajes-texto-argentina-alertan-estafas-paso-protegerse_0_XqOTdOYj2B.html

52. An autonomous government agency responsible for managing the personal data database of Peruvian citizens.

53. David Solar Silva, "Reniec niega hackeo masivo y denuncia al Mininter como responsable del uso indebido de datos", Infobae (April 4, 2025). Available at: <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 (June 5, 2024). Available at: <https://www.swissinfo.ch/spa/investigacion-una-supuesta-filtracion-de-datos-en-servicio-de-emergencias-de-ecuador-ecu-911/79794108>

A particularly concerning series of incidents affected **public institutions and essential services**, exposing the personal information of millions of people. In **Paraguay**, two massive data breaches—one involving the Superior Court of Electoral Justice, which affected more than 7 million people, and another involving public financial institutions and more than 17,000 records—exposed highly sensitive data, including political affiliation, employment information, and public officials’ salaries⁵⁵.

In **Uruguay**, multiple data breaches affected government agencies, including the exposure of nearly 15,000 visa applications—mostly from migrants and refugees—citizen service databases containing more than 574,000 records, and more than 13,000 credentials for accessing government systems^{56 57 58}. In **Honduras**, meanwhile, journalistic investigations documented the circulation of voter registration data and millions of phone numbers on illegal marketplaces⁵⁹.

Data breaches affecting sectors such as **healthcare and education** were among the period’s most serious impacts. In **Argentina**, more than 665,000 medical records of patients treated at clinics and hospitals were put up for sale. The data ranged from X-rays, ultrasounds, and CT scans to laboratory test results⁶⁰. In **El Salvador**, personal data on nearly one million people enrolled in the social security system was leaked, along with 50 GB of information from educational institutions and 141 GB from debt collection agencies^{61 62 63}. In **Chile**, a ransomware attack on a university led to the release of 46 GB of data, including personal and financial information on students and university staff⁶⁴. In **Mexico** and **Brazil**, attacks on public educational institutions exposed the data of thousands of students, many of them under the age of 18, thereby increasing the risks faced by children and adolescents^{65 66}.

55. TEDIC, “Filtraciones masivas en Paraguay: cuando nuestros datos quedan a la deriva”, TEDIC (March 31, 2025). Available at: <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 (March 27, 2025). Available at: <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 Agescic: se filtran correos y números de teléfono de más de 574.000 registros”, la diaria (February 11, 2025). Available at: <https://ladiaria.com.uy/politica/articulo/2025/2/agescic-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 (July 26, 2024). Available at: <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 (June 3, 2024). Available at: <https://www.laprensa.hn/premium/honduras-ciberseguridad-datos-hondurenos-venta-sitios-web-robo-AJ19674958>

60. Juan Brodersen, “Hackean ‘Informe Médico’, un proveedor de software de Argentina y venden resultados de estudios de pacientes”, Clarín (April 4, 2025). Available at: 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 (September 17, 2024). Available at: <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 (January 7, 2025). Available at: <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 (April 3, 2025). Available at: <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 (November 14, 2024). Available at: <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 (April 8, 2025). Available at: <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 alunos em site de empresa condenada”, Intercept Brasil (August 13, 2024). Available at: <https://www.intercept.com.br/2024/08/13/governo-de-alagoas-despeja-dados-de-alunos-e-professores/>

Across the board, the documented incidents show that data breaches do not end with the initial exposure of data. Instead, they are often amplified through the **circulation and monetization of data on dark web forums**, where information is sold or released in bulk. During the period under review, for example, the sale of approximately 250,000 bank records belonging to individuals in **Brazil** was documented for amounts equivalent to a few credits within these markets⁶⁷, as well as the sale of access credentials to tax systems in **Mexico**—including electronic signature credentials—belonging to at least 111,000 taxpayers⁶⁸.

In **Argentina** and **Venezuela**, databases containing millions of personal records were offered for sale, along with partial samples that let buyers verify the information's authenticity before purchasing the full datasets^{69 70}.

This resale ecosystem **is not limited to specialized forums**. A growing trade in personal data was also observed on everyday platforms, particularly Telegram. The Derechos Digitales investigation, *Identities for sale: The illegal trade in Latin American personal data on Telegram*⁷¹, documented the operation of groups and channels on the platform dedicated to the illegal buying and selling of personal data in various Latin American countries, where addresses, phone numbers, health information, political affiliations, and other sensitive data circulate easily and at low cost.

Data breach incidents show how the repeated exposure of personal information has become normalized across the region, fostering a dangerous **sense of inevitability**. Yet behind every leaked database are not merely technical records, but people whose rights are compromised. These impacts are not evenly distributed: women, children and adolescents, LGBTIQ+ people, human rights defenders, and historically marginalized communities face heightened risks of harassment, fraud, digital violence, and persecution when their information is exposed.

From a technical standpoint, implementing measures such as least privilege, data encryption, access logging, multi-factor authentication, and periodic reviews of what data is stored and for how long is not only a best practice but also an organizational obligation. Several of these measures must be integrated from the start of system development, following the principle of privacy by design, which treats data protection not as an added feature but as a consideration from the outset.

67. Felipe Payão, "Dados bancários de 250 mil brasileiros são vazados em fórum criminoso", TecMundo: Tudo sobre Tecnologia, Entretenimento, Ciência e Games (November 27, 2024). Available at: <https://www.tecmundo.com.br/segu-ranca/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 (December 19, 2024). Available at: <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 (January 5, 2025). Available at: <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] (April 30, 2025). Available at: <https://x.com/vesinfiltro/status/1917532243846705173>

71. Available at: <https://www.derechosdigitales.org/recursos/identidades-en-venta-el-mercado-ilegal-de-compra-y-venta-de-datos-personales-latinoamericanos-en-telegram/>

3.4. Disinformation During Elections

Disinformation has become a strategic tool in Latin American electoral processes. In contexts marked by polarization and a demand for immediate information, the circulation of false or misleading content—in the form of text, images, videos, or audio—seeks to stir emotions to influence voting behavior, benefit or harm candidates, and erode trust in the electoral process. Monitoring electoral processes in the region reveals patterns that combine **traditional tactics and technological innovations**, making organized disinformation a structural component of political competition. During the period under review, elections were held in Brazil, Chile, Ecuador, Mexico, Uruguay, and Venezuela, with the following trends emerging.

A recurring tactic is to **sow doubt about the integrity of the electoral process through “evidence” that appears technical**—screenshots, figures, videos—but is actually misinterpreted or taken out of context. Those spreading disinformation exploit the public’s limited understanding of electoral procedures to present minor incidents or human errors as evidence of orchestrated fraud.

In **Mexico**, for example, claims that there were “duplicate tally sheets” in the PREP⁷² went viral as alleged evidence of fraud, even though the PREP provides preliminary and informational results and is subject to data-entry or digitization errors that are later corrected during the official vote count⁷³. Similar narratives emerged in **Ecuador**, based on misleading visual “evidence”: a video circulated claiming that the electoral authority was distributing pens whose ink would fade to alter votes. However, the footage was taken out of context and actually came from another country and another year^{74 75}.

After the election, an image went viral claiming that the OAS had declared the results illegitimate, even though an official statement had validated the process⁷⁶.

Even temporary outages of institutional websites—such as those reported by the Electoral Institute of Mexico City during election day and the delayed updates on

72. The Preliminary Election Results Program (PREP) is a computer system implemented by the electoral authorities that provides preliminary election results on the very night of Election Day, based on a quick count of the tally sheets received from the polling places.

73. Regina López Puerta y Ave Velázquez, “Video desinforma sobre supuesto fraude electoral con actas duplicadas”, El Sabueso (June 11, 2024). Available at: <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 (April 8, 2025). Available at: <https://lupa.com.ec/verificaciones/cne-esferos-borrrables-elecciones-2025/>

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

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

Chile's Servel⁷⁷ website—were reinterpreted as signs of manipulation and used to sow doubt about the integrity of the process^{78 79}.

At the same time, a consistent pattern of **impersonation** has emerged through accounts and posts that imitate media outlets to make rumors appear as confirmed news. In Venezuela, TikTok profiles designed to look like news programs spread unverified claims as facts, such as the alleged arrest or escape of the president of the National Electoral Council. The repetition of these claims across multiple accounts amplified their visibility, created confusion, and was later exploited to discredit the independent press and reinforce pro-government narratives⁸⁰.

In **Ecuador**, monitoring identified impersonation through fabricated content that replicated the logos and visual styles of media outlets and public institutions to project legitimacy. Under this guise, messages designed to trigger fear or outrage—for example, falsely linking migration to crime or promoting nonexistent scholarships—were disseminated in visual formats designed for quick consumption, whether through paid advertising or screenshots designed to go viral without being questioned⁸¹.

Along the same lines, fake screenshots attributed to political figures and videos reused out of context circulated to promote false narratives or create the appearance of nonexistent irregularities. In **Venezuela**, fake screenshots circulated on X showing María Corina Machado applauding an attempted coup in Bolivia⁸². In **Mexico**, a video from 2021 showing a person voting with a gun was repurposed as if it were from the 2024 election⁸³. In both cases, the appearance of authenticity was enough for the content to go viral before any verification could take place, taking advantage of the immediacy of social media consumption.

A qualitative shift in electoral disinformation came with the **widespread adoption of artificial intelligence tools**, which make it possible to create highly realistic content at low cost and at a speed previously unimaginable. Deepfakes—video or audio manipulations that make it appear that a person said or did something that never happened—have become particularly effective because they transform a false narrative into audiovisual “evidence” that is easy to share. In **Venezuela**, for example, a deepfake circulated in which an AI-generated voice was overlaid onto a real video of political leader Delsa Solórzano to make her say that candidate

77. The Chilean Electoral Service is an autonomous state agency with constitutional status, responsible for organizing, administering, and overseeing electoral and plebiscite processes.

78. Cristóbal Palacios, “Lentitud en publicación de resultados: Servel informa desfase en actualización en su sitio web”, La Tercera (October 28, 2024). Available at: <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 (June 4, 2024). Available at: <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 Tiktak posicionan rumores y facilitan propaganda oficialista”, Cazadores de Fake News (October 21, 2024). Available at: <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 (April 9, 2025). Available at: <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 (July 12, 2024). Available at: <https://cotejo.info/2024/07/fb-falso-maria-corina-machado-no-felicitó-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 (June 4, 2024). Available at: <https://verificado.com.mx/desinformaciones-que-marcaron-jornada-electoral/>

Edmundo González “never won” the election⁸⁴. Audios presented as WhatsApp “leaks” and attributed to María Corina Machado were also circulated; after being verified, they turned out to be false and AI-generated⁸⁵.

In **Brazil**, disinformation took on an explicit gender bias. At least five deepfake attacks targeting female candidates were documented: fake images or videos in which a woman’s face is superimposed onto nude bodies to create sexualized content⁸⁶. This content seeks to degrade and intimidate, directly linking disinformation to gender-based violence in the political sphere.

At the same time, the cases show that **disinformation often operates in a coordinated manner across multiple platforms**⁸⁷. In **Brazil**, a study of far-right political groups during the 2024 municipal election campaign found that 17% of the links shared on WhatsApp contained disinformation, compared with 7% on Telegram⁸⁸. In **Venezuela**, networks of accounts that cite one another and pose as opposition members were documented amplifying narratives on X and TikTok, while other layers of the operation used Telegram for coordinated harassment⁸⁹. This approach became even more sophisticated in Ecuador, where paid advertising was added to the mix: companies registered in the United States reportedly used Google products to spread disinformation ads targeting candidates⁹⁰.

3.5. Targeted Attacks

Targeted attacks consist of deliberate actions against specific digital infrastructures, systems, or services. Rather than operating “at random,” they involve selecting previously identified targets and carrying out actions designed to achieve a specific purpose, such as gaining access, disrupting services, extorting, or committing fraud. This section describes various types of targeted attacks identified across the region, including phishing campaigns, account takeovers, app-based fraud, and attacks against digital infrastructure.

84. Edy Pérez Alvarado, “Está alterado el video donde Delsa Solórzano dice que Edmundo González Urrutia ‘jamás ganó las elecciones’”, Cotejo.info (December 4, 2024). Available at: <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 (June 4, 2024). Available at: <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 (November, 2024). Available at: <https://desinformante.com.br/wp-content/uploads/2024/11/AI-in-the-2024-brazilian-elections.pdf>

87. Anna Bentes, “Elections, digital rights, and disinformation: challenges and lessons learned from the Brazilian experience in 2022”, Derechos Digitales (November, 2023). Available at: <https://www.derechosdigitales.org/en/recursos/elections-digital-rights-and-disinformation-challenges-and-lessons-learned-from-the-brazilian-experience-in-2022/>

88. Redação Desinformante, “Pesquisa aponta que desinformação circula mais em grupos de extrema direita no WhatsApp que no Telegram”, desinformante (January 28, 2025). Available at: <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 (August 26, 2024). Available at: <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 (April 9, 2025). Available at: <https://lupa.com.ec/explicativos/desinformacion-electoral-ecuador-2025/>

Although these techniques are used in different contexts, it is important to note that the same tools and attack vectors can also be used against activists, journalists, human rights defenders, and civil society organizations. Understanding how these attacks operate helps us assess the risks different actors face in the digital environment and the impacts these incidents can have on people's daily lives and the functioning of key institutions.

Financial gain remains one of the main drivers of cyberattacks in the region. Methods have become increasingly diverse and sophisticated, as illustrated by the **proliferation of banking trojans**⁹¹ designed for the Latin American context. Infranus, detected primarily in **Mexico**, evolved from spyware⁹² into a banking trojan with a distinctive capability: it can modify the victim's clipboard to silently replace the account number to which money is being transferred, diverting funds to criminals⁹³. In **Colombia**, campaigns targeting public agencies and companies used remote access trojans distributed via highly tailored phishing emails⁹⁴ impersonating banks and messaging services; opening the attachment installed software capable of keylogging, capturing screenshots, and stealing credentials⁹⁵.

Another growing form of attack involves **loan apps**, which combine social engineering⁹⁶ with extortion and prey on economic vulnerability. In **Ecuador**, the Digital Autonomy Center (CAD)⁹⁷ describes how this practice is expanding by exploiting limited access to employment and formal credit. These apps offer quick loans through streamlined approval processes, but once installed, they request intrusive permissions—contacts, photo gallery, location, camera, and call logs—which then become the basis for coercion. After the loan is granted, they impose exorbitant interest rates and impossible repayment deadlines; any delay triggers threats, defamation targeting the borrower's contacts, and, in some cases, intimidation through personal or intimate photos, location tracking, and even the creation of additional, unsolicited “debts”⁹⁸.

91. Banking Trojans are a type of malware that secretly installs itself on the victim's device with the aim of stealing login credentials. Their name comes from the analogy with the Trojan horse, as they masquerade as legitimate programs to deceive users and get themselves installed.

92. Spyware is a type of malware that is secretly installed on a device to collect information about a user without their knowledge or consent—such as passwords, messages, location, or screen activity—and send it to third parties.

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

94. Phishing is a deceptive technique used to obtain confidential information (such as login credentials or banking information) by impersonating a legitimate entity or a trusted individual. It is carried out through fake but seemingly official communications, such as emails, text messages (smishing), or phone calls (vishing), which direct the victim to fraudulent websites designed to steal their data or infect their device with malware.

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

96. Social engineering is a set of manipulation techniques used to deceive people into revealing confidential information, performing specific actions, or granting access to secure systems. Unlike purely technical attacks, social engineering exploits trust, fear, curiosity, or a lack of knowledge.

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

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

In **Mexico**, the Citizen Council reported more than 1,000 apps of this kind as of 2024, several of which were still active on Google Play⁹⁹. In **Peru**, the Superintendency of Banking and Insurance warned about at least 17 apps using the same scheme¹⁰⁰.

Meanwhile, identity **impersonation** has become a critical link in the digital fraud chain. Phishing remains one of the most common attack vectors. In **Honduras**, Indigenous organizations and land defenders have been targeted by personalized phishing campaigns impersonating international donors to obtain work schedules and map contact networks, to facilitate physical persecution by non-state actors and extractive companies¹⁰¹.

This same vector is also used for financial fraud. In **Chile**, messages warning that points from a popular loyalty program in the fuel sector were about to expire directed recipients to a website nearly identical to the official one, where they were asked to provide banking information to cover a supposed shipping fee¹⁰². In **Colombia**, a similar scheme impersonated the National Tax and Customs Authority (DIAN) through fake debt notices¹⁰³. AI amplifies this type of scam by enabling more personalized, convincing messages, reducing the effectiveness of traditional detection cues.

When a scam succeeds in obtaining credentials, account theft becomes a tool for scaling up the fraud. In the **Dominican Republic**, the list of victims includes President Luis Abinader, whose X account was compromised, as well as ministers and the president of the Senate; in several cases, attackers used the accounts to solicit money from contacts, exploiting the trust associated with the impersonated identity¹⁰⁴. In **Honduras**, a gang used phishing to gain access to WhatsApp accounts and then offered dollars at low prices; victims transferred money to accounts controlled by the scammers¹⁰⁵.

A more complex technique is SIM swapping, which exploits weaknesses in SMS verification to impersonate an individual to their mobile carrier and transfer their phone number to a SIM card controlled by the attacker, thereby gaining access to the verification codes that protect bank accounts and other services. In **Brazil**, a criminal organization activated more than 180 SIM cards using third-party data to transfer ownership of phone lines, gain access to bank accounts, and carry out

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 (January 28, 2025). Available at: <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 (August 22, 2024). Available at: <https://www.sbs.gob.pe/>

101. Fundación Acceso, “Observatorio Centroamericano de Seguridad Digital: Informe interanual 2020-2025 [Manuscript in progress].

102. Génesis Friz, “‘Tus puntos van a caducar’: Phishing, la tentadora estafa que llega por SMS y cómo no caer en ella”, BioBioChile (April 7, 2025). Available at: <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 (August 24, 2024). Available at: <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 (July 9, 2024). Available at: <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 (October 14, 2024). Available at: <https://www.elpais.hn/asi-operaba-la-banda-de-ciberataque-a-cuentas-de-whatsapp-en-honduras/>

fraudulent transfers¹⁰⁶. **Costa Rica** set a legal precedent when the Superintendency of Telecommunications ordered Claro to compensate a customer who fell victim to SIM swapping, finding that the carrier failed to fulfill its obligation to verify the identity of the person requesting a replacement SIM card¹⁰⁷. The ruling places the responsibility of telecommunications companies to protect their customers, beyond simply providing the service, at the center of the debate.

Meanwhile, a wave of incidents struck **government institutions and essential services**, undermining the state's ability to provide services and maintain operations. Ransomware¹⁰⁸ emerged as a central threat in this area. In **Uruguay**, attackers encrypted the departmental government's data—including backups—and demanded \$650,000 in bitcoin, rendering digital services inoperable and forcing reconstruction efforts¹⁰⁹. In **Paraguay**, the Ministry of Education and Culture suffered an attack that took all of its online portals and services offline, with the attackers demanding \$1 million¹¹⁰. In **Argentina**, a company responsible for distributing credit cards and official documents was hit by ransomware, putting personal data at risk of exposure¹¹¹.

Incidents with political implications were also reported. In Bolivia, the e-Government Agency reported hundreds of attacks on government websites toward the end of 2024, and one of the most high-profile incidents compromised the Senate's website, whose homepage was replaced with messages and symbols—an attack known as defacement^{112 113}. In **Brazil**, on the same day that Judge Alexandre de Moraes ordered X to be blocked, the Federal Supreme Court and other government institutions were hit by simultaneous cyberattacks¹¹⁴. The timing of the attacks and the fact that they also targeted the agency responsible for implementing the block suggest a coordinated action in response to the court ruling. In **Costa Rica**, unauthorized access to an institutional email account at the University of Costa

106. Assessoria de Comunicação – PCDF, “PCDF desarticula organização criminosa especializada no golpe do Sim Swap”, Polícia Civil do Distrito Federal (February 12, 2025). Available only from Brazil or via a VPN with a server located in Brazil: <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 (January 10, 2025). Available at: <https://semanariouniversidad.com/pais/sutel-ordena-a-claro-indemnizar-por-e2%82%a16-millones-a-victima-de-sim-swapping/>

108. Ransomware is a type of malware that blocks access to a computer system or encrypts the victim's files, demanding payment of a ransom (usually in cryptocurrency) in exchange for unlocking them. Once infected, the device displays a message on the screen with payment instructions, usually accompanied by a countdown timer that increases the pressure on the victim.

109. El Observador, “Intendencia de Paysandú sufrió ataque informático y hackers pidieron US\$ 650 mil para recuperar información”, El Observador (July 26, 2024). Available at: <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 (October 22, 2024). Available at: <https://www.infobae.com/america/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 (June 21, 2024). Available at: https://www.clarin.com/tecnologia/empresa-logistica-ocasa-sufrio-ciberataque-ransomware-web-caida_0_AhR2VtSgrd.html

112. Defacement is a type of attack that involves gaining unauthorized access to a website and modifying its visible content, replacing the home page with images and/or messages chosen by the attacker.

113. Redacción El Deber, “Incrementan los hackeos a páginas del Estado y expertos advierten riesgos para la población”, El Deber (August 17, 2024). Available at: 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 (September 3, 2024). Available at: <https://www.elperiodista.cl/2024/09/tribunal-supremo-de-brasil-sufrio-ciberataque-en-medio-de-polemica-por-x/>

Rica allowed a bomb threat to be sent, forcing the evacuation of the campus¹¹⁵.

Targeted attacks across the region show that public institutions and companies that handle sensitive information or provide essential services are the main targets and therefore also bear a central responsibility for digital security. When critical infrastructure or systems that manage data fail, the risks are not limited to financial fraud; they can also affect people's safety, access to services, and the ability of citizens—including journalists, activists, and civil society organizations—to participate in public life. In contexts where civil society organizations and human rights defenders rely on these platforms to access public information or file complaints, service disruptions can also hinder accountability processes and access to rights.

115. Erick Murillo, "UCR confirma que hackearon correo para enviar amenazas de bomba", CR Hoy (September 30, 2024). Available at: <https://crhoy.com/tecnologia/ucr-confirma-que-hackearon-correos-para-enviar-amenazas-de-bomba/>

4. Thematic Areas



4 Thematic Areas

This section provides a systematic overview of the information gathered from various sources and levels of evidence. It draws on data and case documentation and incorporates experiences shared by OLAD member organizations, as well as common patterns and concerns identified through the Observatory's collaborative work during the period covered by this report.

This chapter explores four thematic areas that emerged particularly strongly from regional discussions and the materials reviewed: technology-facilitated gender-based violence, the exploitation of biometric data, internet shutdowns, and surveillance.

The analysis that follows combines quantitative evidence with the situated knowledge of the organizations, offering a broad yet detailed view of how these threats affect the lives of people and communities defending rights across Latin America.

4.1. Technology-Facilitated Gender-Based Violence

Technology-facilitated gender-based violence (TFGBV) is one of the most persistent and evolving threats in Latin America. Far from being isolated incidents, it stems from a range of mechanisms used by perpetrators—whether individuals or groups—to harass, control, humiliate, sexualize, extort, or harm women and LGBTIQ+ people because of their gender or identity, using platforms, devices, algorithmic systems, and personal data.

During the period covered by this report, OLAD organizations documented both the persistence of established forms of aggression and the emergence of new forms, demonstrating perpetrators' ability to adapt to emerging technologies and the sociopolitical contexts of each country. The spread of AI tools and cases that gained public attention in different countries confirm that this violence is not simply a collection of incidents, but a structural phenomenon that takes shape within new technical infrastructures and social contexts.

Organizations that operate hotlines for victims of TFGVB in the region—such as the S.O.S. Digital Center run by Fundación InternetBolivia.org in Bolivia and Navegando Libres, run by Taller de Comunicación Mujer in **Ecuador**—have been instrumental in shedding light on the dynamics of this type of violence and, above all, in providing direct support to those affected¹¹⁶.

4.1.1. Navegando Libres

In the case of the **Navegando Libres** helpline, cases in Ecuador reveal the persistence of established forms of TFGVB¹¹⁷. These include sexual extortion, defamation, the dissemination of intimate content, harassment, identity theft, and unauthorized access to accounts. Many of these cases are linked to relationship breakups, family conflicts, or reprisals against women involved in feminist and social activism.

Alongside these recurring patterns, the organization identified particularly serious emerging forms of violence. One of these is violence facilitated by loan apps: in one documented case, a woman who applied for a loan through an app had her contacts accessed without her knowledge and, after falling behind on payments, both she and her family members received threats, intimidating messages, and manipulated images containing humiliating content.

According to the organization, this phenomenon should be understood in the context of economic insecurity, which disproportionately affects women in Ecuador, who face higher unemployment and greater family and caregiving burdens, as well as gender digital divides that limit their understanding of how these types of apps work and of digital security practices.

There were also several reported cases in which perpetrators invoked criminal gangs to heighten fear in sextortion situations, as well as threats from former partners with ties to state-owned security companies, revealing how TFGVB is intertwined with power structures and privileged access to surveillance technologies.

116. To learn more about these organizations' work on technology-facilitated gender-based violence, see the resources available at: <https://tcmujer.org/> y <https://internetbolivia.org/>

117. For more details on the concept and forms of TFGVB according to international human rights standards, see: Derechos Digitales, "Combating Technology-facilitated Gender-based Violence (TFGBV) through the Lens of International Human Rights Law." Available at: <https://www.derechosdigitales.org/en/recursos/combating-technology-facilitated-gender-based-violence-tfgbv-through-the-lens-of-international-human-rights-law/>

Through its work with a feminist collective, the organization also documented a case of mass dissemination of intimate content in Telegram groups. Members of the collective attempted to infiltrate these groups and identified that one of the requirements for joining was to share sexual content involving female relatives or acquaintances. Once this requirement was met, they faced other verification mechanisms they could not access for security reasons, suggesting an organized, tiered structure for disseminating this type of violence.

Documentation and support efforts are also affected by platform decisions. The temporary suspension of Navegando Libres' Instagram account—which the organization links to changes in Meta's policies¹¹⁸—highlights how platforms can, through action or inaction, undermine critical support infrastructure for people experiencing digital violence.

4.1.2. S.O.S. Digital

Quantitative data from Fundación InternetBolivia.org's **S.O.S. Digital Center** reinforces this regional analysis and offers a different view of the problem's scale. The helpline recorded 377 reported cases of digital violence during the period. Sexual abuse involving ICTs (29.5%) and harassment (21%) were the most common forms of violence, together accounting for nearly half of all cases.

Along with these, other forms of violence also occur consistently, such as discrediting (10.5%), hacking (10%), misuse of information (9.5%), threats (9.5%), and fraud (7%). This shows that TFGBV is not limited to a single set of aggressive behaviors but instead manifests through multiple, combined forms.

The cases also show that women continue to be the most affected, and that most cases are concentrated among those aged 25 to 54, followed by those aged 18 to 24 and, to a lesser extent, adolescents aged 13 to 17. This pattern suggests that, although digital violence affects different age groups, it has a particularly strong impact on young and adult women during stages of their lives marked by high levels of social, professional, emotional, and community exposure.

The helpline's response goes beyond the technical dimension. Throughout the reporting period, the most frequent forms of support were emotional support, legal guidance, and technical guidance, with emotional support accounting for a slightly larger share. This is significant because it shows that TFGBV causes harm that cannot be addressed solely through technical aspects of digital security or platform management; it also requires legal responses and sustained support.

118. Throughout 2025, Meta implemented changes to its moderation policies that particularly affected content related to gender, sexual diversity, and sex education, leading to suspensions and restrictions on the accounts of feminist and human rights organizations in several countries in the region.

4.1.3. Other cases

Beyond the work of OLAD organizations, public sources from various countries identified cases of TFGBV. The first involves the circulation and amplification of misogynistic discourse on digital platforms, often driven by algorithmic dynamics. In **Brazil**, an investigation by Núcleo and AzMina showed how TikTok progressively exposes teenage boys to far-right content and narratives that degrade women¹¹⁹. In the same country, Brasil Paralelo launched a large-scale anti-abortion advertising campaign on Meta that combines targeting, emotional appeals, and an ultraconservative agenda that also extends to issues of gender and sexual diversity¹²⁰.

A second pattern is the persistence of digital sexual violence as a mechanism of coercion, humiliation, or blackmail. This dynamic is evident in cases of sextortion reported on dating apps in **Mexico**, where perpetrators first build a relationship of trust and then threaten to disseminate intimate images to obtain money¹²¹. It is also observed in **Ecuador**, in the case of a man accused of contacting a teenage girl on WhatsApp to request sexual images after gradually escalating the tone of his messages¹²².

A third, particularly concerning pattern is the use of AI to sexualize, discredit, or expose women without their consent. In **Bolivia**, attacks against women in politics included insults about their bodies, sexual insinuations, and deepfakes intended to undermine their public legitimacy¹²³. In **Mexico**, this same dynamic affected public figures, including a senator and a streamer, through the dissemination of sexual deepfakes without their consent^{124 125}. In **Chile**, a student was accused of creating sexual deepfakes of his female classmates, highlighting the extent to which these tools are already available and can be used to cause harm without requiring advanced technical knowledge¹²⁶.

This last pattern is directly linked to the findings of **a study on deepfake apps in**

119. Flávia Santos and Sofia Schurig, “Como o TikTok alimenta a misoginia entre adolescentes brasileiros”, Núcleo Jornalismo (April 3, 2025). Available at: <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 (June 21, 2024). Available at: <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 (February 12, 2025). Available at: <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”, Teleamazonas (November 6, 2024). Available at: <https://www.teleamazonas.com/hombre-detenido-ciberacoso-adolescente-ecuador/>

123. Marcelo Blanco, “Insultos, montajes y amenazas: La guerra silenciosa contra las mujeres en la política boliviana”, Bolivia Verifica (April 25, 2025). Available at: <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 (October 16, 2024). Available at: <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, May 27, 2025, <https://www.infobae.com/mexico/2025/05/27/alana-flores-es-victima-del-deepfake-y-anuncia-acciones-legales-contra-usuario/>

126. Génesis Friz and Valeska Belmar, “Acusan a alumno de 8° básico de crear imágenes sexuales de compañeras con IA en San Pedro de la Paz”, BioBioChile (April 25, 2025). Available at: <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>

Latin America. Based on automated data collection from Google Play, the study identified 105 apps available as of December 2024. The study concluded that 89.5% of these apps pose a potential threat to women¹²⁷.

The findings show that these tools are neither difficult to find nor use. On the contrary, platforms such as Google Play legitimize this ecosystem by enabling the widespread distribution of technologies that facilitate symbolic and sexual forms of abuse without consent, under lucrative business models. This is compounded by their ease of use, sexualized promotional images, misleading age ratings, and a widespread lack of transparency about the origins of many of these apps. This ecosystem is the result of business decisions that prioritize profitability over the safety of women and LGBTIQ+ people, turning platforms into complicit actors in gender-based violence.

4.2. Exploitation of Biometric Data

Data exploitation refers to contexts in which people's personal information, particularly when it involves sensitive data, ceases to be merely information about them and becomes a resource from which others derive economic or strategic benefits. It is not simply a matter of a company collecting information, but of asking under what conditions it does so, what is obtained in return, how much people understand about how their data is processed, and whether they retain any ability to make decisions or, later on, regain control over their data.

With biometric data, the issue becomes even more sensitive. Unlike a password, the iris, face, or fingerprints cannot be changed if they are compromised, and their processing can have lasting effects.

The case of World, formerly Worldcoin, illustrates this issue. To understand the institutional responses described below, it is necessary to briefly look back at what happened in 2023. Starting that year, long lines began to form in several cities across Argentina in front of devices that scanned the irises of those who approached. In exchange, the company offered the equivalent of between \$30 and \$50 in cryptocurrency¹²⁸. In August of that year, 9,500 people in Argentina had their irises scanned in a single day (one person every nine seconds), amid annual inflation exceeding 115%¹²⁹.

The phenomenon was repeated in other countries in the region with economies under pressure, such as Ecuador, Chile, Peru, Colombia, and the Dominican Repu-

127. Ximena Cuzcano-Chavez and 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>

128. York Perry, "Worldcoin bate récord en Argentina pese a los riesgos y 9.500 personas se registran en un día", *FayerWayer* (September 5, 2023). Available at: <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* (August 31, 2023). Available at: <https://www.diariobitcoin.com/argentina/worldcoin-record-argentina-9-500-registros-dia/>

blic¹³⁰. Behind these lines was Worldcoin, a project co-founded by Sam Altman—also the founder of OpenAI¹³¹—whose implementation in Latin America was led by Tools for Humanity (TFH). The project offers a digital identity based on iris scanning, with the promise of creating a global system that can distinguish humans from bots online. Building on this case, this section examines how biometric data can become a source of value for companies, and why this has raised concerns among authorities, courts, and civil society organizations.

World operates in two stages: registration and the subsequent use of the digital identity. During registration, the user downloads the World App and provides information such as their name, phone number, email address, bank account, and device metadata. They must then go in person to a device called an Orb, which scans their iris to complete verification. Based on those images, the system generates an iris code—a numerical representation of iris texture—and compares it with previously generated codes to check whether that person has registered before. If the code is unique, the system creates a digital credential called World ID¹³².

The company maintains that it does not store the iris image as a photograph, but instead transforms it into codes and fragments¹³³ to reduce its direct exposure. However, this does not eliminate the underlying problem: even if the image is not circulated as a photograph, biometric data remains the system's foundation because verifying uniqueness depends on it. The data changes form, but it remains indispensable¹³⁴.

Once registration is complete, using World ID no longer requires a new scan. According to the company, the system uses cryptographic tools to let users prove they are part of a group of verified individuals without having to reveal their biometric data or civil identity again. That is the project's promise: to let users prove they are a “unique human” across various digital services without re-exposing their original biometric data¹³⁵.

To reinforce this privacy promise, the system incorporates mechanisms such as data fragmentation, secure multi-party computation, and zero-knowledge proofs (SMPC and ZKPs, respectively). In simple terms, these techniques are designed to ensure that no part of the system has full access to the iris code and that certain verifications can be performed without revealing the underlying information.

This technical architecture does not, however, eliminate the underlying tensions.

130. Pedro Martín Sánchez, “El caso de Worldcoin y la alerta de las autoridades con criptomonedas”, *Diario Libre* (November 16, 2024). Available at: <https://www.diariolibre.com/economia/negocios/2024/11/16/el-caso-de-worldcoin-y-la-alerta-de-las-autoridades-con-criptomonedas/2913636>

131. Wikipedia, “Worldcoin”, (April 11, 2026). Available at: <https://es.wikipedia.org/w/index.php?title=Worldcoin&ol-did=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 (January 23, 2025).

133. These codes are known as IrisCode, binary representations generated from unique iris patterns using an encoding algorithm. Unlike a password, this code cannot be changed if it is compromised, since it is derived directly from an immutable physical trait.

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 (January 23, 2025).

135. Ibid.

One concerns consent: in several countries, registration was promoted through financial incentives, making the idea of a fully voluntary choice more complicated, particularly when most registrants were people experiencing economic hardship, willing to provide irreplaceable data in exchange for a few dollars' worth of cryptocurrency. The question is not simply whether a person consented, but under what conditions they did so and how much they actually understood about the processing of their biometric data.

Another tension concerns long-term risk. Even when the company promises anonymization or data fragmentation, doubts remain about what it really means to delete biometric data once it has been captured, transformed, and linked to a digital credential. The system's complexity compounds this risk. A technical audit in March 2025 identified multiple vulnerabilities in World's cryptographic circuits, including flaws that could allow an attacker to register multiple times by bypassing the uniqueness mechanism¹³⁶. Although the company resolved the most serious issues, the audit also warned of unresolved statistical risks. These vulnerabilities reinforce concerns about the security of a system that handles irreplaceable data.

Questions also remain about who actually controls that data and for what purposes. The promise that the data "is not used for other purposes" relies largely on corporate claims and technical mechanisms that are difficult to audit independently.

These concerns were not merely conceptual. In several countries across the region, World's deployment triggered institutional responses that clarify the model's problems. In **Brazil**, the National Data Protection Authority (ANPD) opened a formal investigation into World Foundation and TFH's processing of biometric data. The investigation focused on the large-scale collection of sensitive data and how the company obtained consent. The key issue was that registration was incentivized through financial compensation in cryptocurrency, which could undermine the freedom of consent, especially given the sensitive and irreversible nature of the data. In January 2025, the ANPD ordered the suspension of the financial compensation and required transparency measures, including appointing a data protection officer.

The company attempted to modify its model through an invitation-based scheme, in which the reward was no longer tied to the scan itself but to bringing in new users. However, the authorities considered that the risks persisted and maintained the restrictions, including the possibility of daily fines.

In **Chile**, during 2024, the National Consumer Service (SERNAC)¹³⁷ raised concerns about the lack of clear information regarding the purposes of data processing, the associated risks, and the entities that could access the data, shifting the discussion toward consumer rights. Shortly thereafter, the Supreme Court ruled in favor

136. Least Authority, "Security Audit Report Worldcoin", Least Authority (March 7, 2025). Available at: <https://leastauthority.com/wp-content/uploads/2025/03/Least-Authority-Worldcoin-MPC-Circuit-Final-Audit-Report.pdf>

137. It is the Chilean government agency responsible for protecting and promoting consumer rights, ensuring compliance with regulations, and initiating legal action on behalf of consumers.

of a protection action filed by the mother of a teenager whose iris had been scanned¹³⁸. The court ordered the removal of the minor's World ID and all records of his biometric data, emphasizing that, since he was under 18 years of age, there was no valid consent from his legal representatives. The ruling was clear: the company should not have collected the data without verifying his age and obtaining the required consent.

Another study by Fundación Amaranta adds a situated and gender-based perspective to this scenario¹³⁹. Based on interviews, the study shows that those who had their irises scanned were predominantly women who were mothers facing urgent financial needs. It also reveals that, in many cases, people did not understand what the company did with their data, what risks that processing entailed, or how feasible it was to delete that information later. The study confirms that precariousness, gender inequalities, and information asymmetries shape the problem and undermine the possibility of a truly free decision.

The World case also raised concerns in countries across the region beyond Brazil and Chile. In **Peru**, the ANPD investigated the company amid public debate over the security of biometric data and the legality of the model involving iris scans in exchange for cryptocurrency^{140 141}. In the **Dominican Republic**, Pro Consumidor ordered the company to cease operations after identifying potentially unfair contract terms and issues with its duty to provide information, the lack of a local registered office, and the processing of biometric data in exchange for an economic benefit¹⁴². In **Ecuador**, the project's rollout also faced public criticism and closures due to a lack of permits, amid warnings from organizations and experts about a lack of transparency among partner companies and institutional weakness in effectively overseeing such practices¹⁴³.

These cases show that, despite its technical sophistication, World's model leaves key questions unanswered about the validity of consent, effective control over data, applicable jurisdiction, and the risks associated with a potential breach of biometric information. Behind every scanned iris is a person who could not foresee the consequences of that exchange.

138. SERNAC, "SERNAC denuncia ante la Justicia a Worldcoin por recolección indebida de datos biométricos", Servicio Nacional del Consumidor (August 28, 2024). Available at: <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 (January 2, 2025). Available at: <https://amarantas.org/wp-content/uploads/2025/01/ong-amaranta-datos-biometricos.pdf>

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 (June 3, 2024). Available at: <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 (June 3, 2024). Available at: <https://www.gob.pe/institucion/anpd/noticias/965752-minjurdh-supervisa-la-recopilacion-de-datos-personales-por-worldcoin>

142. Comunicaciones Pro Consumidor, "Pro Consumidor suspende las operaciones de Worldcoin en República Dominicana", Pro Consumidor (November 15, 2024). Available at: <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 (September 18, 2024). Available at: <https://labarraespaciadora.com/worldcoin-datos-biometricos/>

4.3. Internet shutdowns

An internet shutdown, also known as an internet blackout or internet blocking, is an interruption in connectivity that prevents full or partial access to the internet in a given area. It can result from intentional or accidental causes and affect places ranging from local areas, such as a city, to broader regions, including entire countries. The duration varies and can range from minutes to several days, depending on the cause and scale¹⁴⁴.

Unlike the cases documented in the chapter on Censorship, where specific websites or platforms are restricted, internet shutdowns affect connectivity itself. Their consequences interfere with the right to seek and disseminate information, limit freedom of expression, hinder access to basic services such as health care and education, and, in emergencies, can isolate entire communities at the time they most need to communicate.

The causes can vary widely. **Intentional shutdowns** occur when an actor—usually a state actor—deliberately interrupts (or orders the interruption of) connectivity, generally to control the flow of information during protests or elections. **Collateral shutdowns** occur when the internet goes down as a result of another event, such as an energy crisis, without anyone having directly ordered it, but with the same practical effect on people. A third type includes cases in which the disconnection results from years of **deteriorating infrastructure**, without any specific event triggering it.

During the period covered by this report, Latin America recorded cases of all three types in Venezuela, Ecuador, Chile, Panama, Cuba, and Colombia. The analysis combines technical documentation from OLAD member organizations—including Conexión Segura, through its **VE Sin Filtro** monitoring initiative in Venezuela, and Fundación Karisma, through K+Lab's **Observatorio de Bloqueos de Internet** (OBI) in Colombia—with a systematic analysis of public cases documented by media outlets and global monitoring initiatives.

Among the **intentional shutdown** cases documented in the region, the one in **Panama** stands out. In June 2025, the government suspended internet access and mobile phone service in Bocas del Toro province for nearly two weeks in response to social mobilizations against a social security reform¹⁴⁵. The measure was implemented under a state-of-emergency declaration.

A year earlier, VE Sin Filtro documented a connectivity outage in **Venezuela** that affected only CANTV and Movilnet, the two main state-owned operators, for nearly

144. Coop La Lonja, "Corte De Internet: Ataque A La Libertad De Expresión", Coop La Lonja (January 12, 2012). Available at: <https://cooplalonja.com.ar/corte-de-internet/>

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

two hours, leaving several states without service¹⁴⁶. No official explanation was provided, and although it is not possible to confirm the outage was intentional, it occurred four days after the July 28, 2024 presidential election, amid an escalation of website blocking. The lack of official transparency surrounding the incident is itself part of a pattern.

Collateral shutdowns in the region during this period were primarily caused by energy crises that disrupted connectivity. **Ecuador** was the first country to face them, as a severe drought that affected hydroelectric plants—which account for 72% of the country’s electricity generation¹⁴⁷—triggered power outages lasting up to 14 hours a day and left several provinces without internet access for months¹⁴⁸. In **Venezuela**, meanwhile, a collapse of the national power grid on August 30, 2024, left the country without connectivity for nearly 21 hours, with 8 out of 10 people losing internet access¹⁴⁹. The government attributed the blackout to opposition sabotage, the same narrative it repeated in the following months whenever the power grid collapsed again¹⁵⁰.

Cuba accounted for the largest number of incidents during this period. Between October 2024 and March 2025, the country experienced four national power grid failures that disrupted connectivity. The first, caused by a thermal power plant failure, left 10 million people without power or internet access¹⁵¹. This was followed by damage from Hurricane Rafael in November¹⁵², another failure in December, and yet another in March 2025, all stemming from the same causes: fuel shortages and obsolete, poorly maintained infrastructure¹⁵³. **Chile** experienced its own incident when a massive power grid failure left 14 of the country’s 16 regions without power, disrupting internet and mobile phone service for more than 12 hours in what was the country’s largest blackout since 2010¹⁵⁴.

In **Colombia**, Karisma’s OBI documented two outages in the province of Chocó in August 2024. The first lasted between 6 and 12 hours¹⁵⁵ and coincided with a

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

147. Wikipedia, “Ecuadorian blackouts”, (April 5, 2026). Available at: https://en.wikipedia.org/wiki/2024_Ecuadorian_blackouts

148. Freedom House (2025), “Ecuador: Freedom on the Net 2025 Country Report”, Freedom House (2025). Available at: <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). Available at: https://vesinfiltro.org/res/files/informe-presidenciales_2024-VEsinFiltro.pdf

150. Wikipedia, “Venezuelan blackouts, 2024”, (February 22, 2026). Available at: https://en.wikipedia.org/wiki/2024_Venezuelan_blackouts

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

152. Dikytan and IODA, “Cuba enfrenta apagones y cortes de internet tras falla de la red eléctrica nacional”, IODA (November 27, 2024). Available at: <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 (March 14, 2025). Available at: <https://elpais.com/america/2025-03-15/un-nuevo-apagon-deja-a-cuba-a-oscuras-en-su-peor-tesis-energetica-en-decadas.html>

154. The Associated Press, “A Sweeping Power Blackout Leaves Most of Chile in Darkness”, Houston Public Media (February 26, 2025). Available at: <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 (November 28, 2024). Available at: <https://obi.karisma.org.co/2024-10-28-colombia-microcaida-quibdo-choco-agosto-2/>

torrential storm that disrupted the power supply; the second lasted between 3 and 6 hours¹⁵⁶. These incidents also occurred in a context of precariousness: only 13% of the population has internet access, mainly in the departmental capital, meaning any outage affects a community that already has very limited access.

A third type of shutdown occurs through a gradual loss of connectivity due to **infrastructure deterioration**. Cuba clearly illustrates this dynamic, as between October and December 2024, the country ranked last in the world in download speed with an average of 2.96 Mbps, which was insufficient even for basic tasks such as video calls or standard-quality video streaming, which require at least 10 Mbps¹⁵⁷. As of May 2025, speeds had improved only slightly to 3.35 Mbps, keeping the country near the bottom of the global index¹⁵⁸. Decades of underinvestment, exacerbated by an economic blockade that has limited access to technology and external financing, and reliance on a single state-owned company have resulted in obsolete infrastructure that fails to provide even minimal connectivity for the population.

This is compounded by the restriction on unlimited internet packages priced in Cuban pesos, as ETECSA¹⁵⁹ has prioritized payments in U.S. dollars for services offered since May 2025, introducing packages priced in foreign currency and setting limits on consumption in the national currency¹⁶⁰. As a result, any data plan beyond the basic allowance costs more than the country's monthly minimum wage, making connectivity an economic privilege beyond the reach of those without access to foreign currency¹⁶¹. Cuba is not technically disconnected, but for those without foreign currency, the difference in practice from an actual shutdown is minimal.

4.4. Surveillance

Digital surveillance is the monitoring, interception, collection, and analysis of online data carried out by state or private actors to control or neutralize individuals deemed of interest¹⁶². In Latin America, this practice has historically targeted human rights defenders, continuing a legacy of surveillance that has persisted since colonial times. What for decades took the form of physical surveillance or telephone wiretaps is now accompanied—though not replaced—by new forms of

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

157. Diktyon, "Censura de Internet en Cuba: Informe número 7", Diktyon (2024). Available at: 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). Available at: <https://www.speedtest.net/global-index/cuba>

159. Cuban Telecommunications Company S.A (ETECSA)

160. Orlando González, "ETECSA Incrementará Tarifas y Dolarizará Servicios en 2025", Guardianes Digitales (2025). Available at: <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 (June 6, 2025). Available at: <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). Available at: https://www.acceso.or.cr/wp-content/uploads/2021/08/2020_Art_Herramientas_Vigilancia_CA-mayo2020.pdf

surveillance deployed on people's devices, through facial analysis, and through the monitoring of their words online, often imperceptible to those subjected to them, making these methods effective tools of control and repression.

Digital surveillance in Latin America took various forms that reflect the expansion of state control over people's lives across the region. Among the documented trends are the use of spyware against journalists and activists; forced physical access to devices during arrests or police operations; the deployment of facial recognition systems, mass video surveillance, and large-scale data analysis platforms; and cyberpatrolling on social media.

During the period covered by this report, OLAD organizations documented these phenomena from different angles. **Fundación Acceso** investigated the psychosocial effects of spyware on affected people in Central America and documented key surveillance trends through the Central American Observatory for Digital Security. Meanwhile, **Conexión Segura**, through its VE Sin Filtro monitoring initiative, documented the deployment of surveillance technologies in Venezuela during the 2024 electoral process. These contributions are complemented by cases documented by media outlets, helping to build a regional picture of the phenomenon.

Further evidence of spyware use emerged during this period. In **Mexico**, court documents from the litigation between WhatsApp and the Israeli company NSO Group—the manufacturer of Pegasus spyware—revealed in April 2025 that 456 people were targeted with this software between April and May 2019 during the administration of Andrés Manuel López Obrador, making **Mexico** the country with the highest number of victims out of a total of 1,233 identified globally¹⁶³. The Ministry of National Defense signed a contract to acquire Pegasus in April of that same year, and the system's final operator was to be the Military Intelligence Center, a secret agency whose existence the armed forces have repeatedly denied.

In 2024, the United States confirmed that it funded the use of Pegasus in **Colombia** for counternarcotics operations during Iván Duque's administration, providing \$11 million¹⁶⁴. Although the official U.S. account maintained that Duque was not informed, experts and a criminal complaint challenged that version, arguing that an agreement of that magnitude could hardly have been made without the executive branch's knowledge^{165 166}.

In **Ecuador**, the National Assembly decided in December 2024 to initiate an over-

163. R3D, "Gobierno mexicano usó Pegasus para espiar al menos a 456 personas en 2019", R3D: Red en Defensa de los Derechos Digitales (April 14, 2025). Available at: <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 (November 8, 2024). Available at: <https://es.wired.com/articulos/estados-unidos-confirma-que-financio-el-uso-del-software-espia-pegasus-en-colombia>

165. July Sánchez Cristo, "Expertos en ciberseguridad dicen que es casi imposible que Duque no supiera del software Pegasus", Cambio Colombia (November 16, 2024). Available at: <https://cambiocolombia.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 (September 25, 2024). Available at: <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/>

sight process following allegations that Daniel Noboa's government used Pegasus to monitor journalists, opposition figures, and activists. However, as of the publication of this report, the process had produced no public results¹⁶⁷.



Beyond the numbers, people bear the consequences of every surveillance technology. In April 2025, **Fundación Acceso** published a study exploring the concrete impacts of this type of surveillance through interviews with human rights defenders and journalists from **Central America** who had been infected with spyware¹⁶⁸. The interviewees described effects that began with initial panic and evolved into prolonged states of constant alertness, anxiety, insomnia, and depression. Several people changed their routes, stopped frequenting certain places, altered their social media habits, and switched to more secure messaging apps. Some even ended up in exile.

The impact also extended to work teams: when someone reveals that they were under surveillance, it can trigger a chain reaction of panic, forcing teams to devote time and resources to security rather than their advocacy work. It also has an economic impact, including new devices, psychological therapy, and relocation costs.

In this context, Fundación Acceso developed a comprehensive support guide for people who provide digital protection assistance to those affected by spyware and other surveillance technologies¹⁶⁹.

In Central America, the Central American Observatory for Digital Security¹⁷⁰, launched by Fundación Acceso, documented several critical trends between 2024 and 2025¹⁷¹. In **Guatemala** and **Nicaragua**, physical access to devices has allowed prosecutors' offices and governments to construct "conspiracy" narratives by using legitimate encrypted tools as alleged evidence of criminal activity.

Specifically, Daniel Ortega's government in **Nicaragua** has consolidated a multi-layered surveillance infrastructure. Since 2017, a system has been operating at a military base in Managua that combines radio direction-finding—capable of locating phone signals—with the SORM-3 system, which allows interception of calls,

167. Richard Josue Jimenez Mora, "Pegasus: la Asamblea fiscalizará supuesto espionaje del Gobierno", *Diario Expreso* (December 17, 2024). Available at: <https://www.expreso.ec/actualidad/asamblea-pegasus-espionaje-224876.html>

168. Olga Paz, "Estudio de impactos y afrontamientos psicosociales ante ataques digitales", Fundación Acceso (April, 2025). Available at: 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 (July 30, 2025). Available at: <https://pasalavoz.acceso.or.cr/guia.html>

170. Systematic recording and analysis of digital security incidents affecting human rights defenders, journalists, and civil society organizations in Central America. Available at: <https://www.acceso.or.cr/observatorio-centroamerica-no-de-proteccion-digital/>

171. Fundación Acceso, "Observatorio Centroamericano de Seguridad Digital: Informe interanual 2020-2025 [Manuscript in progress]".

messages, emails, social media activity, and bank transactions¹⁷². Added to this is the transnational persecution of exiles in **Costa Rica** through doxxing and social media monitoring¹⁷³.

In **Venezuela**, Conexión Segura documented the deployment of various surveillance technologies during the electoral process¹⁷⁴. The organization identified a phishing campaign targeting opposition supporters through a fake form that collected personal data such as addresses. The malicious link was promoted through fake accounts on X, Instagram, TikTok, and Telegram. In addition, drones were used to capture images of protests, focusing on participants' faces, which government spokespeople later disseminated.

The organization also documented reports of illegal phone searches during police operations, in which officers demanded that devices be unlocked so they could inspect WhatsApp conversations and search for terms associated with opposition political figures. The government also instrumentalized its VenApp -originally designed to report failures in public services- to channel anonymous reports against protesters through the submission of photographs and geolocation data, allowing authorities to locate those reported.

Another trend is the expansion of surveillance technologies in public spaces, **such as mass video surveillance and facial recognition**. In Brazil, São Paulo implemented the Smart Sampa system in late 2024, a video surveillance and facial recognition initiative with the stated goal of identifying fugitives and preventing crime by cross-referencing images in real time with judicial databases. The system has involved the installation of 40,000 cameras in public and private spaces across the municipality¹⁷⁵. More than 8% of those arrested through Smart Sampa had to be released due to errors: an 80-year-old retiree was detained for hours because the system identified him as a sex offender; a psychiatric patient was handcuffed at a mental health facility because of an outdated arrest warrant. Civil society organizations also noted that official data do not record the racial identity of more than half of those detained, making it impossible to assess whether the system engages in algorithmic racism.

172. Redacción Confidencial, "Centro de espionaje ruso opera en base militar de Mokorón en Managua", Confidencial (August 26, 2024). Available at: <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 [Manuscript in progress]".

174. VE sin Filtro, "Redes de control: Censura y represión digital en las elecciones presidenciales en Venezuela", VE sin Filtro (2024). Available at: 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 (March 17, 2026). Available at: <https://elcomercio.pe/mag/historias/smart-sampa-la-revolucionaria-pero-polemica-red-de-vigilancia-digital-en-sao-paulo-nnda-nnrt-noticia/>

The system's expansion also reached educational settings, as nearly 400 Smart Sampa cameras were installed in municipal schools in São Paulo, where facial recognition is used in access areas to generate biometric records of students, teachers, and staff without clear privacy policies or informed consent mechanisms for people under 18¹⁷⁶.

There are multiple initiatives to deploy facial recognition technology in **Brazil**. These included the installation of 17 facial recognition checkpoints in Rio de Janeiro during the 2024 New Year's celebration on Copacabana Beach¹⁷⁷, as well as the deployment of 12 additional facial recognition cameras, drones, and 18 checkpoints on access roads during Lady Gaga's free concert on the same beach in May 2025, which drew more than 2.5 million people^{178 179}.

In **Argentina**, Javier Milei's government created the Artificial Intelligence Unit Applied to Security, which empowers federal forces to monitor social media and the dark web, analyze real-time camera footage using facial recognition, use algorithms to "predict" future crimes, create suspect profiles, and patrol large areas with drones¹⁸⁰. In May 2025, the National Intelligence Plan revealed that the Secretariat of State Intelligence aimed to monitor actors who caused a "loss of confidence in economic policies" or "manipulated public opinion" during electoral processes¹⁸¹.

In **Paraguay**, the digital rights organization TEDIC documented the expansion of facial recognition cameras installed since 2018 by at least 13 public institutions, with no legal framework regulating their use to date, no human rights impact assessments, and with funds from the Universal Service Fund diverted to finance surveillance infrastructure¹⁸². In **Ecuador**, a presidential decree issued in September 2024 stipulated that ECU-911 assume exclusive control of local government cameras and implement a real-time video surveillance system using facial and license plate recognition¹⁸³.

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

177. Marianela Milanes, et al., "Reconocimiento facial y tecnologías de vigilancia en América Latina: casos, proveedores y dinámicas comerciales", Al Sur (June, 2025). Available at: <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] (May 2, 2025). Available at: https://www.instagram.com/derechos_digitales/p/DJKKV6ARFF4/

179. Douglas Corrêa, "Seguridad reforzada para concierto de Lady Gaga en Copacabana", Agência Brasil (April 29, 2025). Available at: <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 (July, 2024). Available at: <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 (May 25, 2025). Available at: <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 (April 29, 2025). Available at: 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 (September 18, 2024). Available at: <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>

Another form is the use of large-scale data analysis platforms. **Ecuador** formalized a collaboration with Palantir Technologies between January and May 2025¹⁸⁴ ¹⁸⁵ to implement its data analytics platform within the National Customs Service (SENAE), with the stated goal of combating smuggling and customs fraud. Palantir is a U.S. company whose technology—originally developed for U.S. government intelligence operations—enables large-scale cross-referencing of data from multiple sources to identify patterns and profiles of individuals in real time. The contract authorizes SENA to consolidate data from other public entities on Palantir’s platform¹⁸⁶, thereby expanding data processing beyond customs control and posing significant risks to people’s privacy and their control over their own data.

Finally, another aspect of digital surveillance documented in the region is the monitoring of speech on social media. **Derechos Digitales** documented two practices employed by governments in the region¹⁸⁷: profiling, which involves categorizing social media users based on whether their posts are favorable, critical, or opposed to the government; and cyberpatrolling, which involves covertly monitoring online activity to identify and prosecute individuals for their online activities. Both operate on the assumption that any content published online is freely available for use by the state, even for purposes of persecution, an assumption that human rights organizations have challenged¹⁸⁸.

In Colombia, an investigation revealed that the government hired a company to improve its public image; in practice, this led to a list of 486 X users classified as favorable, neutral, or opposed to the government. In Brazil, a federal government tender to contract social media profiling services came to light in 2024; the government justified it as a tool to measure its popularity, analyze users’ emotions using AI, and combat disinformation¹⁸⁹.

In **Mexico**, a 2024 investigation based on documents leaked by the Guacamaya collective revealed that the Ministry of Defense acquired the Israeli HIWIRE software in 2020 to monitor social media users critical of the military in real time, map their interactions, and create fake accounts to interact with the targets covertly¹⁹⁰.

Cyberpatrolling has spread across the region with varying levels of regulation and opacity. In **Uruguay**, the General Directorate of Police acknowledged in 2024 that

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 (May 29, 2025). Available at: <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”, ECUAVISIA (January 23, 2025). Available at: <https://www.ecuavisa.com/politica/el-gobierno-anuncio-respaldo-de-google-palantir-y-healthbird-para-la-transformacion-digital-de-ecuador-20250123-0102.html>

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). Available at: 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* (May 9, 2025). Available at: <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). Available at: https://www.derechosdigitales.org/wp-content/uploads/Informe-RELE-vigilancia-masiva_cerrado.pdf

190. Ibid

it monitored social media. That same year, a teenager was arrested after being mistakenly identified as a participant in clashes at educational institutions, having been confused with someone of the same name on social media¹⁹¹.

In other countries, cyberpatrolling has been incorporated into or reinstated in regulatory frameworks. In Argentina, it was reinstated in local regulations in 2024 after having been repealed in 2022; in Paraguay, it was incorporated into the law on the reform and modernization of the National Police in June 2024¹⁹².

191. Ibid

192. Ibid

5. Conclusions



5 Conclusions

count for this context risk offering partial responses: protecting a device does not fully protect a person whose organization is being persecuted by the state, nor a journalist whose media outlet has been shut down. Understanding this dimension is essential for digital security responses to be truly effective.

The report also highlights a troubling tension between the rapid adoption and legitimization of surveillance technologies and practices and the slow pace at which transparency and rights-protection mechanisms are advancing. In particular, efforts to legally validate practices such as cyberpatrolling or expand state analytical and surveillance capabilities are occurring without corresponding, proportionate oversight and accountability mechanisms.

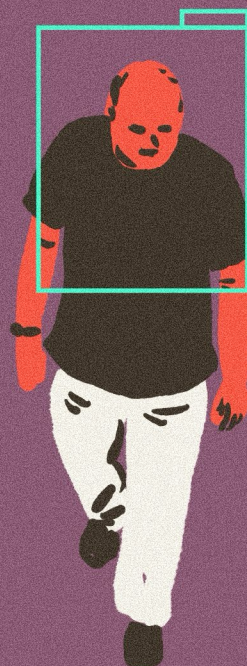
One aspect that distinguishes this report from its previous edition is the growing presence of AI as a cross-cutting vector in the documented incidents. Its inclusion across multiple sections reflects the challenge of understanding AI not only as a tool for innovation, but also as part of broader infrastructures of power, classification, control, and the production of harm, whose effects do not fall equally on everyone. A clear example is the generation of sexualized deepfakes, which has become a form of violence and control directed particularly at women. However, it is important to note that these new technologies do not replace more traditional forms of repression and control. In Central America, for example, multiple mechanisms persist that combine technological tools, restrictive legal reforms, and political persecution, operating simultaneously and reinforcing one another.

Throughout this report, it becomes clear that the impacts of these incidents are not distributed evenly. Journalists, activists, political opponents, women, LGBTIQ+ people, migrant communities, people living in poverty, and people with limited access to digital resources face specific risks depending on the type of technology or attack. In several cases, the impact extends beyond the individual and produces collective effects, such as self-censorship, the chilling of protest, weakened support networks, or shrinking civic space.

The unequal distribution of these impacts can be attributed to both state and private actors. For instance, state actors use surveillance software to persecute political opponents. Meanwhile, in the private sector, notable examples include World, which buys biometric data on a massive scale, and lending apps that use extortion mechanisms. Both cases illustrate how technology is used to exploit people's economic circumstances.

Finally, the elimination of funding by the U.S. government and the closure of USAID in 2025¹⁹⁴ had a significant impact on civil society organizations in the region. This situation hampered the coordination of OLAD's work and delayed the publication of this report. Nevertheless, the sustained support of its members was essential to bringing this report to completion, and we would like to thank them for their collaboration in developing *In Focus 2*.

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



 Derechos
Digitales
AMÉRICA LATINA

