

The background of the entire page is a dark purple. Overlaid on this are stylized, high-contrast illustrations of ten diverse people in various 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 tracking or selection box. The people 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 in a wheelchair, a man in a white t-shirt and black pants looking down, a woman in a white dress, a man in a black t-shirt and black shorts, a woman in a white shirt and black pants, a man in a white shirt and black pants with a backpack, and a woman in a white shirt and black pants.

Na mira 2: um panorama das ameaças digitais na América Latina

Na mira 2: um panorama das ameaças digitais na América Latina

Esta publicação foi produzida pela Derechos Digitales, uma organização independente sem fins lucrativos, fundada em 2005, cuja missão é a defesa, promoção e desenvolvimento dos direitos fundamentais em ambientes digitais na América Latina.

Supervisão geral: Rafael Bonifaz

Coordenação e revisão: Rafael Bonifaz e Jamila Venturini

Análise e redação: Ximena Cuzcano

Pesquisa: Ximena Cuzcano

Revisão de estilo: Gastón Wahnish

Tradução ao português: Dafne Melo

Design: Diego Lepián

Este relatório é o resultado de um trabalho conjunto realizado no âmbito do Observatório Latino-Americano de Ameaças Digitais (OLAD), uma aliança de organizações latino-americanas que inclui Código Sur (regional), Colnodo (Colômbia), Conexión Segura (Venezuela), Derechos Digitales (regional), Escola de Ativismo (Brasil), Fundación Acceso (regional), Fundación InternetBolivia.org (Bolívia), Fundación Karisma (Colômbia), Instituto Nupef (Brasil), LaLibre.net Tecnologías Comunitarias (Equador), MariaLab (Brasil), Social TIC (México), Sursiendo (México) e Taller de Comunicación Mujer (Equador).

Agosto 2026

Como citar esta publicação: Direitos Digitais. (2026). En la mira 2: um panorama das ameaças digitais na América Latina.

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



Esta obra está licenciada sob uma Licença Internacional Creative Commons Atribuição 4.0.
<https://creativecommons.org/licenses/by/4.0/deed.es>

Sumário

1 Introdução	4
2 Metodologia	7
3 Contexto da segurança digital na América Latina	10
3.1. Desenvolvimentos normativos	11
3.2. Censura	14
3.3. Vazamentos de dados	18
3.4. Desinformação nas eleições	21
3.5. Ataques direcionados	24
4 Áreas temáticas	29
4.1. Violência de gênero facilitada pela tecnologia	30
4.1.1. Navegando Libres	31
4.1.2. S.O.S. Digital	32
4.1.3. Outros casos	33
4.2. Exploração de dados biométricos	34
4.3. Bloqueios de internet	38
4.4. Vigilância	41
5 Conclusões	48



1. Introdução

1 Introdução

A internet e as tecnologias digitais constituem um espaço central para o exercício dos direitos humanos na América Latina. Por meio delas, as comunidades têm acesso a informações e serviços essenciais, os ativistas se organizam e se articulam, e os jornalistas documentam os abusos de poder e os denunciam. A manutenção de um espaço livre e seguro é condição necessária para o exercício dos direitos fundamentais. No entanto, esse mesmo espaço também se tornou palco de vigilância, censura, violência e controle. Diferentemente dos relatórios de cibersegurança que se concentram nos impactos econômicos e comerciais, este documento busca destacar como as ameaças e os ataques digitais afetam o trabalho da sociedade civil e o exercício dos direitos fundamentais na região.

O relatório *Na mira 2: um panorama das ameaças digitais na América Latina* é resultado de um trabalho liderado pela Derechos Digitales no âmbito do Observatório Latino-Americano de Ameaças Digitais (OLAD), uma aliança de organizações latino-americanas dedicada à defesa dos direitos humanos no espaço digital. O Observatório permite a troca de conhecimentos e experiências relacionados à segurança digital e serve como plataforma para o monitoramento de incidentes sob a perspectiva dos direitos humanos e do interesse público.

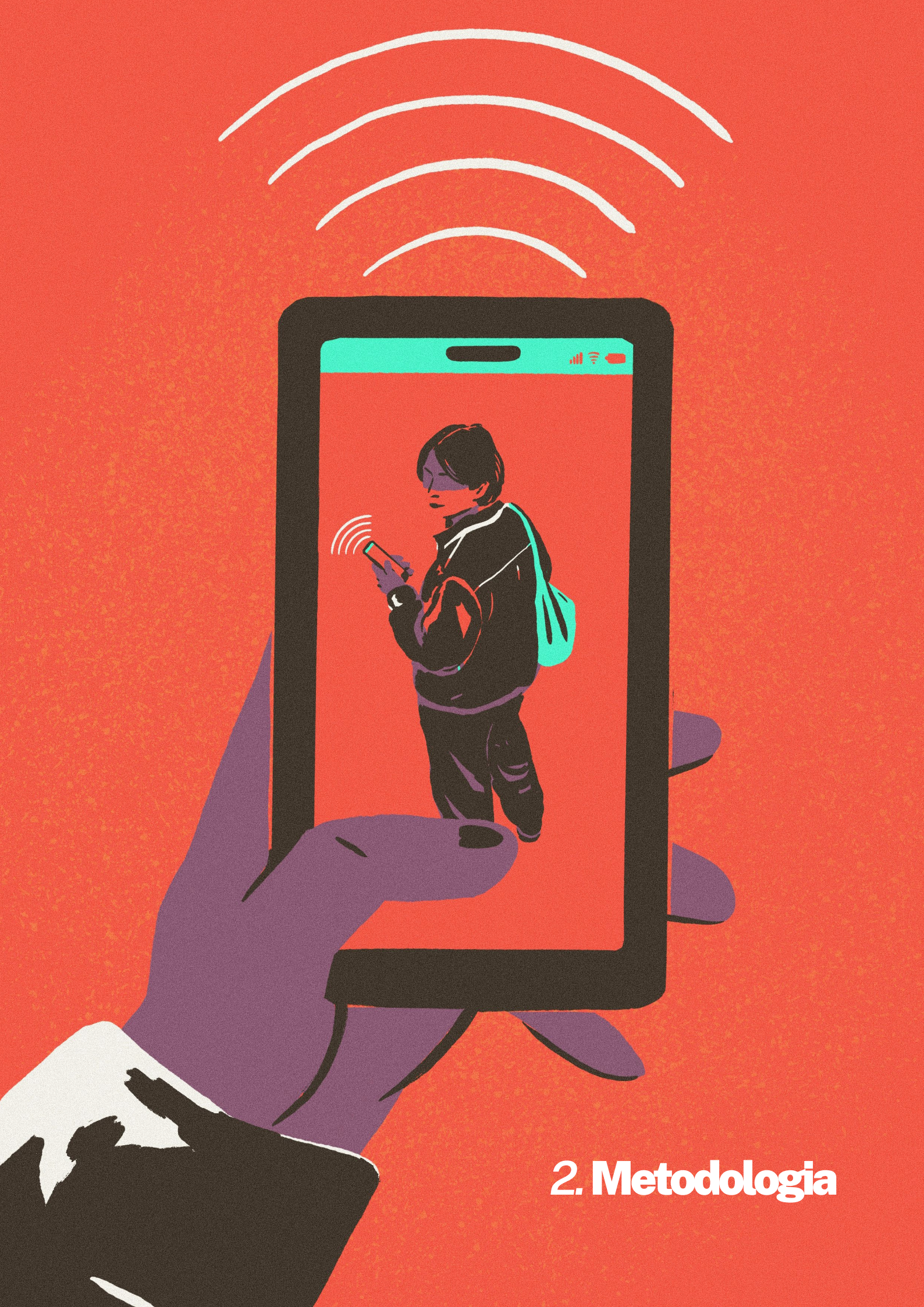
As seguintes organizações fazem parte desta aliança: Código Sur (regional), Colnodo (Colômbia), Conexión Segura (Venezuela), Derechos Digitales (regional), Escola de Ativismo (Brasil), Fundación Acceso (regional), Fundación InternetBolivia.org (Bolívia), Fundación Karisma (Colômbia), Instituto Nupef (Brasil), LaLibre.net Tecnologías Comunitarias (Equador), MariaLab (Brasil), Social

TIC (México), Sursiendo (México) e Taller de Comunicación Mujer (Ecuador). Esta segunda edição se baseou particularmente em relatórios e pesquisas produzidos por várias dessas organizações.

Cada uma das organizações do OLAD tem atuações diferentes de acordo com o contexto do seu país e a sua área de especialização. A partir de diferentes territórios e campos de atuação, eles produzem conhecimento, acompanham casos, investigam ameaças e alertam sobre práticas que afetam os direitos on-line. Derechos Digitales, com base no trabalho de organizações e por meio de monitoramento periódico, conduziu a elaboração deste relatório a fim de destacar como as ameaças digitais afetam o exercício dos direitos na América Latina.

Na mira 2 dá continuidade ao trabalho da primeira edição desta série. Entendemos que a documentação acumulada ao longo do tempo é, em si, uma ferramenta de defesa e de memória. Constitui também um mecanismo essencial para a futura prestação de contas, pois, em contextos autoritários onde não existem hoje condições para investigar, sancionar ou reparar violações, preservar evidências e manter registros rigorosos permite sustentar a verdade dos fatos, fortalecer os processos de justiça — para quando as condições mudarem — e até reduzir o risco de estas agressões ficarem impunes.

O relatório está organizado em duas grandes seções. A primeira, *Contexto da segurança digital na América Latina*, oferece um panorama regional através de cinco eixos: os desenvolvimentos regulatórios do período, a censura em ambientes digitais, os vazamentos de dados, a desinformação em processos eleitorais e os ataques direcionados. A segunda seção, *Áreas temáticas*, aprofunda quatro tendências de incidentes digitais durante esse período: vigilância, exploração de dados biométricos, apagões de internet e violência de gênero facilitada pela tecnologia.



2. Metodologia

2 Metodologia

O relatório *Na mira 2* apresenta um panorama regional dos incidentes de segurança digital que afetam o exercício dos direitos humanos na América Latina. O período de análise abrange de junho de 2024 a maio de 2025. Para efeitos deste relatório, são considerados incidentes os eventos relacionados com a utilização, o controle ou o abuso de tecnologias digitais que geram impactos em direitos como a liberdade de expressão, a privacidade e a proteção de dados, o acesso à informação, a integridade e a segurança de indivíduos e coletivos, bem como a participação cívica em ambientes digitais.

As informações analisadas foram coletadas por meio de duas vias complementares. Em primeiro lugar, foi realizado um monitoramento semanal sistemático de fontes abertas, principalmente notícias publicadas em meios de comunicação, relatórios disponíveis na internet e acompanhamento de incidentes de vazamento de dados disponíveis on-line. Essa abordagem permite a identificação de tendências regionais e a documentação de incidentes com visibilidade pública; no entanto, apresenta limitações relevantes. A cobertura da mídia é desigual entre os países; muitos incidentes não chegam a ser publicados e, em contextos de censura ou fragilidade da imprensa, uma parte significativa dos fatos permanece fora do registro público.

Em segundo lugar, o relatório incorpora informações e análises das organizações que compõem a OLAD, as quais trabalham diretamente no acompanhamento a pessoas e organizações afetadas por ataques digitais, investigando e/ou monitorando este tipo de incidente na região. Essa articulação nos permite preencher as lacunas no monitoramento de notícias e compreender dinâmicas que nem sempre são visíveis em fontes abertas. No entanto, essa via também enfrenta limitações, já que nem todos os casos podem ser tornados públicos

sem aumentar os riscos para as pessoas afetadas ou para aqueles que acompanham os processos. Consequentemente, os achados do relatório não devem ser interpretados como um ranking de incidentes nem como uma medição comparativa entre países, mas sim como uma análise situada de padrões e dinâmicas regionais.

Durante o período analisado, essas limitações foram exacerbadas por um ambiente global cada vez mais adverso para a sociedade civil. Diversas organizações enfrentam restrições ao espaço cívico, níveis crescentes de vigilância e estigmatização de seu trabalho, bem como dificuldades de sustentabilidade financeira, em um contexto de redução ou congelamento de fundos internacionais destinados a projetos nas áreas de direitos humanos e tecnologia. Essas condições afetam diretamente a capacidade de monitorar e documentar os casos continuamente e devem ser consideradas na interpretação dos achados do relatório.

Por fim, as informações coletadas foram organizadas em linhas temáticas que permitem a análise de padrões e tipos de incidentes em nível regional. Em todos os casos, foi aplicado um critério de verificação razoável, priorizando a rastreabilidade das fontes e evitando conclusões que não pudessem ser sustentadas por evidências publicamente disponíveis. Além disso, o relatório adota uma abordagem de não causar danos, evitando cuidadosamente a publicação de detalhes que possam facilitar a revitimização ou riscos adicionais para os indivíduos e comunidades afetados.



3. Contexto da segurança digital na América Latina

3

Contexto da segurança digital na América Latina

Este capítulo oferece uma visão geral do contexto de segurança digital na América Latina durante o período analisado, com base em um processo de sistematização e análise de monitoramento de fontes abertas. Em vez de apresentar um inventário exaustivo de incidentes, busca situar os principais fenômenos observados na região e compreender como eles se manifestam de forma transversal, diferenciando os impactos em diferentes países e grupos sociais.

3.1. Desenvolvimentos normativos

Durante o monitoramento regional, foram identificados desenvolvimentos regulatórios relevantes em diferentes países da América Latina que afetam diretamente o exercício dos direitos humanos no ambiente digital. Nesse contexto, estão surgindo de forma recorrente iniciativas legislativas e regulatórias relacionadas à vigilância estatal, limitações à liberdade de expressão — incluindo mecanismos de censura — e restrições ao acesso à informação pública, entre outras. Esses eixos refletem as respostas estatais que moldam o contexto político e legal que torna possível — e em alguns casos legítima — os incidentes de segurança digital analisados nas seções seguintes.

Cabe ressaltar que os desenvolvimentos regulatórios descritos correspondem ao estado de cada processo legislativo ou regulatório ao final do período analisado. Dado o caráter dinâmico desses processos, algumas iniciativas podem ter avançado, sido modificadas ou arquivadas após essa data, portanto, sua evolução continuará fazendo parte do monitoramento contínuo que dá origem a este relatório.

Uma primeira tendência regulatória observável é a expansão dos marcos regulatórios que ampliam **os poderes de vigilância do Estado** em ambientes digitais, geralmente justificados por discursos de segurança nacional e ordem pública. Na **Argentina**, a Resolução 428/2024 do Ministério da Segurança formalizou um protocolo de prevenção ao delito que permite o monitoramento sistemático de fontes abertas e o uso de tecnologias automatizadas para análise de informações on-line¹. Na data do fechamento deste relatório, o Decreto 383/2025 incorporou o patrulhamento cibernético como uma competência explícita dessa força, sem necessidade de autorização judicial quando se trata de fontes abertas^{2 3}. No **Paraguai**, a Lei 7269/2024 incorporou a vigilância biométrica obrigatória por meio de sistemas de reconhecimento facial em estádios de futebol, estendendo as práticas de monitoramento em massa a espaços públicos⁴. No **México**, diversas iniciativas para reformar a Lei de Segurança Nacional ampliaram, de forma ambígua, a noção de ameaças à segurança, abrindo caminho para uma expansão dos poderes de vigilância do Estado e do controle da informação⁵. No **Ecuador**, a aprovação de uma nova Lei de Inteligência criou um Sistema Nacional de Inteligência com amplos poderes para interceptar comunicações e acessar dados de telecomunicações sem ordem judicial⁶. Na data de fechamento desta publicação, a lei está sob análise do Tribunal Constitucional, após a apresentação de contestações constitucionais que questionam a compatibilidade desses poderes com os direitos fundamentais; no entanto, o Poder Executivo já emitiu as normas de implementação, que autorizam as agências de inteligência a solicitar diretamente informações às operadoras de telecomunicações sobre geolocalização, tráfego de dados e registros de chamadas, sem necessidade de ordem judicial⁷. Na **Venezuela**, a criação, por decreto, do Conselho Nacional de Segurança Cibernética consolidou uma abordagem estatal de vigilância cibernética com amplos poderes, sob uma narrativa de ameaças cibernéticas associadas a redes sociais e atores da oposição⁸.

Por outro lado, na **Colômbia**, foi apresentado o Projeto de Lei 225, que visava reformar a Lei 1621 de 2013 para fortalecer a proteção dos direitos humanos e reforçar o marco legal das agências que realizam atividades de inteligência e contrainteligência, em conformidade com uma decisão da Corte Interamericana de

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

2. República Argentina, “Decreto 383/2025”, Boletín Oficial de la República Argentina (16 jun. 2025). Disponível em: <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 (18 jun. 2025). Disponível em: <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 (12 dez. 2024). Disponível em: <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 (14 out. 2024). Disponível em: <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 (23 jun. 2025). Disponível em: <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 (14 jul. 2025). Disponível em: <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 (21 ago. 2024). Disponível em: <https://elestimulo.com/venezuela/2024-08-21/consejo-nacional-de-ciberseguridad/>

Direitos Humanos⁹. O projeto recebeu parecer favorável para o primeiro debate em novembro de 2024, mas não foi debatido antes do fim da legislatura, sendo, portanto, arquivado¹⁰.

Outra linha regulatória relevante afeta diretamente **a liberdade de expressão e a implementação de mecanismos de censura digital**. Em **El Salvador**, a aprovação da Lei de Segurança Cibernética e a criação da Agência Estatal de Segurança Cibernética (ACE) consolidaram um esquema institucional altamente centralizado com poderes regulatórios, de supervisão e sancionatórios que podem facilitar a remoção de conteúdo on-line¹¹. Na **Colômbia**, o Projeto de Lei n. 023 de 2023, debatido durante 2024, propõe a criação de uma Agência de Segurança Digital com poderes excepcionais para ordenar a paralisação de operações no ciberespaço, o que consiste na interrupção temporária de plataformas ou serviços digitais em contextos definidos como crises. Sua aplicação poderia implicar a suspensão de redes sociais ou mídias digitais e, assim, afetar a circulação de informações¹². Em **Cuba**, a Lei de Comunicação Social, em vigor desde 2024, estabelece um regime abrangente para a regulamentação de conteúdo e mídia digital, reforçando o controle estatal sobre a produção e circulação de informações, afetando particularmente a mídia independente e as expressões não estatais¹³. Na **Nicarágua**, a reforma da Lei n. 1042, a Lei Especial sobre Crimes Cibernéticos, ampliou a classificação de condutas relacionadas à disseminação de informações on-line e estabeleceu um quadro que tem sido usado para sancionar expressões digitais e gerar um efeito inibidor sobre o jornalismo, o ativismo e a sociedade civil¹⁴.

Da mesma forma, observam-se reformas legais que enfraquecem os mecanismos institucionais de **acesso à informação pública**, afetando a transparência e a responsabilização. No **México**, as reformas constitucionais aprovadas entre 2024 e 2025 eliminaram o Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais (INAI) como órgão autônomo¹⁵. Isso limita a capacidade dos cidadãos de conhecer e monitorar as ações do Estado e de participar de maneira informada nos assuntos públicos. Na **Argentina**, as modificações introduzidas em 2024 ao regime de acesso à informação pública ampliaram as causas

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 (1 out. 2024). Disponível em: <https://www.comisionprimeras Senado.com/documentos-pendientes-de-publicacion/ponencias-y-textos-aprobados/4148-ponencia-ple-225-de-2024-inteligencia-y-contrainteligencia/file>

10. De acordo com o Artigo 153 da Constituição Política da Colômbia, as leis estatutárias devem ser processadas e aprovadas em uma única legislatura.

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

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

de reserva e restringiram o escopo do que é considerado informação pública¹⁶. Essa reforma reduz a obrigação do Estado de divulgar informações de interesse público e enfraquece a capacidade de fiscalização cidadã.

Em paralelo, persistem tensões regulatórias em relação à **proteção de dados pessoais**, onde os avanços regulatórios coexistem com estruturas legais que permitem práticas de vigilância. No **Chile**, a aprovação da Lei n. 21.719 sobre a Proteção de Dados Pessoais e da Lei n. 21.663, a Lei-Quadro sobre Segurança Cibernética, fortaleceu o arcabouço institucional nessa área e ampliou os direitos¹⁷. No entanto, esses avanços coexistem com regulamentações que autorizam o uso de tecnologias de vigilância, como dispositivos de interceptação de comunicações (captadores IMSI), no âmbito da legislação antiterrorista¹⁸. Em **El Salvador**, a Lei de Proteção de Dados Pessoais foi implementada paralelamente a um pacote de cibersegurança, no qual os objetivos de segurança nacional e ordem pública são definidos de forma ampla e imprecisa, com salvaguardas institucionais limitadas¹⁹. Isso levanta dúvidas sobre a real primazia dos direitos das pessoas em relação aos objetivos de segurança.

3.2. Censura

O panorama da censura em ambientes digitais na América Latina entre junho de 2024 e maio de 2025 revela um ecossistema de controle cada vez mais adaptável e tecnicamente complexo. Estados têm combinado diversas técnicas de bloqueio de infraestrutura com pressão sobre agentes privados e perseguição legal para criar um efeito sufocante sobre a liberdade de expressão on-line. Essas medidas não são isoladas, mas tendem a ser intensificadas estrategicamente em momentos críticos, como processos eleitorais ou protestos sociais, combinando recursos técnicos com mecanismos institucionais ou coercitivos. Além disso, têm um impacto mais severo sobre jornalistas, ativistas e pessoas com menos recursos técnicos para contornar os bloqueios, aprofundando a exclusão digital e a lacuna no acesso à informação.

Os principais incidentes observados a este respeito são descritos abaixo, organizados por país.

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

17. Juan Carlos Lara, “Los desafíos de la nueva Ley de Protección de Datos Personales”, CIPER Chile (28 jan. 2025). Disponível em: <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 (11 dez. 2024). Disponível em: <https://www.latercera.com/politica/noticia/en-medio-de-tensa-sesion-congreso-aprueba-ley-antiterrorista/BY2SGOUJONH5JHEGFBSLC5LZR4/>

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

Com relação ao **bloqueio de plataformas e redes sociais**, após as eleições de 2024, o governo **venezuelano**, por meio de ordens emitidas pela Comissão Nacional de Telecomunicações (Conatel) aos provedores de internet, implementou uma onda massiva de bloqueios que afetou plataformas como Signal, X, TikTok, Telegram e YouTube^{20 21 22 23}. Até mesmo serviços corporativos como o Microsoft Teams, sites de estatísticas como o Statista e plataformas de entretenimento como Disney+, Max e Amazon Prime Video foram bloqueados²⁴. De acordo com o relatório da VE Sin Filtro, a censura atingiu uma escala particularmente crítica²⁵ entre julho de 2024 e janeiro de 2025, quando foram documentados 79 novos bloqueios de websites, que se somam aos 89 já existentes, muitos deles contra a mídia independente. A isso se soma o bloqueio de sites de provedores de VPN²⁶ como o Proton e o Windscribe, com o objetivo de impedir que os cidadãos burlam as restrições impostas e protejam sua privacidade on-line.

Além disso, a provedora de serviços de internet (ISP, na sigla em inglês) estatal CANTV bloqueou mais de 30 servidores DNS públicos, incluindo os do Google e da Cloudflare²⁷. O DNS funciona como uma “lista telefônica” da internet: ele converte nomes de domínio (por exemplo, o endereço de um site) em números IP que permitem o acesso ao conteúdo. Na prática, a maioria das pessoas usa o DNS fornecido pelo seu provedor de serviços de internet, como a CANTV. Esse controle permite que o provedor restrinja o acesso a determinados sites, impedindo ou manipulando a resolução de DNS. Nessas situações, uma alternativa comum é trocar o provedor de DNS para tentar recuperar o acesso.

Além disso, foram observadas formas de censura destinadas a afetar a disponibilidade dos meios de comunicação. Em agosto de 2024, o site do jornal TalCual sofreu um ataque de negação de serviço distribuído (DDoS, na sigla em inglês), uma técnica que envolve inundar um servidor com tráfego massivo de vários locais para torná-lo inacessível, o que afetou o acesso por aproximadamente quatro horas²⁸.

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

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

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

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

24. Na prática, esses bloqueios geralmente são implementados por meio de interferência técnica, frequentemente no nível do DNS (na resolução de nomes de domínio), para impedir o acesso sem interromper completamente a conexão com a internet.

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

26. Uma Rede Virtual Privada (VPN) é uma ferramenta que criptografa a conexão com a internet e redireciona o tráfego por meio de servidores em outros países, permitindo a navegação de forma privada e que se fure bloqueios ou restrições geográficas impostas pelos provedores de internet.

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

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

No **Brasil**, o Supremo Tribunal Federal ordenou a suspensão total do X devido ao desrespeito reiterado da plataforma às ordens judiciais para nomear um representante legal no país e remover contas ligadas à desinformação. A decisão também estabeleceu penalidades para aqueles que tentaram burlar a suspensão usando VPN. Embora a suspensão tenha fundamento legal no Marco Civil da Internet, seu amplo alcance afetou todos os usuários da plataforma no país, levantando questões sobre sua proporcionalidade em relação aos padrões interamericanos de liberdade de expressão²⁹.

Na **Colômbia**, a entidade estatal Coljuegos — responsável pela regulamentação dos jogos de azar — ordenou aos provedores de internet que bloqueassem o Reddit, considerando que o domínio estava ligado a operadores de jogos de azar não autorizados, com base na Lei n. 1753 de 2015³⁰. O bloqueio foi implementado por meio de redirecionamentos e restrições de DNS, uma medida que foi confirmada por testes independentes realizados com a ferramenta OONI³¹. Embora a medida fosse temporária, levantou dúvidas sobre sua proporcionalidade e a falta de clareza nos critérios utilizados para incluir sites nas listas oficiais de bloqueio³².

Em relação aos **ataques e intervenções na infraestrutura de internet e nos Sistemas de Nomes de Domínio (DNS)** na **Nicarágua**, a Universidade Nacional de Engenharia (UNI), instituição estatal que administra o domínio nacional *.ni*, por meio do NIC.NI, bloqueou arbitrariamente, sem qualquer ordem ou notificação documentada, os domínios de veículos de comunicação independentes como Confidencial, La Prensa, Onda Local e 100% Noticias, forçando-os a migrar para domínios internacionais para continuar operando³³.

Uma tentativa semelhante ocorreu na **República Dominicana**, quando a empresa estadunidense Network Solutions enviou um ultimato ao jornal Listín Diario, exigindo que este apagasse uma edição sobre corrupção, sob ameaça de suspender seu serviço de hospedagem na web³⁴. A empresa alegou violação de seus termos de serviço após receber uma solicitação de remoção³⁵. Este caso destaca o papel que as empresas privadas que operam em níveis de infraestrutura podem desempenhar na imposição de mecanismos de censura indireta, utilizando cláusulas contratuais vagas para silenciar informações de interesse público.

29. Lucía Camacho, “La suspensión de X en Brasil, y la vigencia del Estado de Derecho”, Derechos Digitales (11 set. 2024). Disponível em: <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 (7 jun. 2024). Disponível em: <https://blog.karisma.org.co/las-dudas-que-quedan-tras-el-bloqueo-de-reddit-en-colombia/>

31. OONI é um projeto e um conjunto de ferramentas de software livre desenvolvido pelo The Tor Project, cujo objetivo é monitorar, medir e documentar a censura na internet, a manipulação do tráfego e a interferência em redes de telecomunicações em todo o mundo. Disponível em: <https://ooni.org/es/>

32. Lucía Camacho, “La suspensión de X en Brasil, y la vigencia del Estado de Derecho”, Derechos Digitales (11 set. 2024). Disponível em: <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 (14 mar. 2025). Disponível em: <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 (15 maio 2025). Disponível em: <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 (15 maio 2025). Disponível em: https://listindiario.com/la-republica/20250515/comunicado-listin-diario-censura-digital_857815.html

Em **Cuba**, o Estado utiliza a tecnologia Deep Packet Inspection (DPI)³⁶ para analisar o tráfego em tempo real e bloquear aplicativos de mensagens criptografadas como Signal e DeltaChat³⁷. Essa técnica é agravada por apagões totais e deliberados da internet pela empresa estatal ETECSA durante mobilizações sociais, bem como pelo aumento das tarifas para limitar o acesso da população³⁸.

Também em **Cuba**, em agosto de 2024, uma pessoa foi condenada a um ano e meio de prisão após publicar um meme com imagens de figuras do governo, e pelo menos outras quatro foram presas e interrogadas por publicações em redes sociais³⁹. Entre setembro e outubro, a onda de repressão levou ao fechamento de pelo menos um veículo de comunicação, à intimação para interrogatório e ameaça de prisão para quatro diretores de mídia e à renúncia de pelo menos nove jornalistas e ativistas^{40 41}.

Foram observados casos de perseguição judicial em **Honduras**, onde o veículo de comunicação Hondudiarío foi investigado por “difamação com publicidade” após noticiar, por meio de uma publicação no X, tensões internas nas Forças Armadas⁴². Em **El Salvador**, a Procuradoria-Geral da República preparou mandados de prisão contra jornalistas do El Faro após uma investigação publicada no YouTube sobre pactos do governo com gangues⁴³.

3.3. Vazamentos de dados

Governos e empresas armazenam grandes volumes de dados pessoais para operar serviços, administrar programas e gerenciar procedimentos cotidianos. Quando o processamento de dados é realizado sem padrões adequados de segurança e governança ou com processos de terceirização pouco controlados, a probabilidade de exposição ou acesso não autorizado aumenta. Nesse contexto, o vazamento de dados pessoais tornou-se um dos fenômenos mais recorrentes no cenário da segurança digital na região.

36. Deep Packet Inspection (DPI), em português, Inspeção Profunda de Pacotes, é uma tecnologia de análise de tráfego de rede que, ao contrário dos métodos de filtragem convencionais, permite o exame do conteúdo completo dos pacotes de dados que circulam na internet, e não apenas de sua origem ou destino. Isso permite que o operador de rede identifique e bloqueie seletivamente aplicativos, protocolos ou conteúdo específicos, mesmo quando ferramentas de criptografia são utilizadas.

37. Diktyon, “Informe #6 sobre la salud del Internet en Cuba”, Guardianes Digitales (out. 2024). Disponível em: <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 (1 jun. 2025). Disponível em: <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 (ago. 2024)”, Yucabyte (set. 2024). Disponível em: <https://www.yucabyte.org/2024/09/26/violaciones-de-derechos-digitales-en-cuba-agosto-de-2024/>

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

41. Yucabyte, “Violaciones de derechos digitales en Cuba (out. 2024)”, Yucabyte (27 nov. 2024). Disponível em: <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 «Hondudiarío» por supuesto delito de injuria”, ARTICLE 19 (2 fev. 2025). Disponível em: <https://articulo19.org/unidad-contradelitos-informaticos-de-la-interpol-de-honduras-investiga-a-medio-hondudiarío-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 (9 maio 2025). Disponível em: <https://www.fidh.org/es/region/americas/el-salvador/el-salvador-escalada-de-persecucion-y-ataques-a-la-libertad-de-prensa>

Um vazamento de dados ocorre quando informações pessoais ou confidenciais, armazenadas por entidades públicas ou privadas, são acessadas por indivíduos não autorizados. Isso possibilita seu uso para fraudes, extorsão, vigilância ou violência. Ao contrário de outros tipos de incidentes associados a conjunturas específicas, os vazamentos de dados são resultado de práticas organizacionais deficientes que se repetem em diferentes países e setores, como coleta excessiva de dados, terceirização tecnológica sem controles adequados e mecanismos frágeis de proteção e monitoramento de acesso, em um contexto no qual diversos países da região ainda carecem de marcos regulatórios para a proteção de dados pessoais. Este relatório identificou casos específicos em 12 países⁴⁴, além de vazamentos de âmbito regional.

Um dos tipos mais comuns de vazamento de dados identificados não se devia a ataques cibernéticos sofisticados, mas a erros básicos na proteção da informação. Em particular, vários incidentes tiveram origem em **configurações incorretas**, em que as bases de dados foram deixadas acessíveis sem autenticação. Em termos simples, isso equivale a deixar arquivos confidenciais em um espaço público sem qualquer tipo de fechadura. Na **Colômbia**, o aplicativo de pagamentos GoPass deixou para trás um bucket do Google Cloud Storage⁴⁵, expondo dados de quase um milhão de pessoas, incluindo números de registro de veículos e de identificação fiscal⁴⁶.

Na **Costa Rica**, uma falha de configuração na infraestrutura da Movistar deixou acessíveis aproximadamente 650 mil arquivos, contendo documentos de identidade, autorizações de trabalho e selfies utilizadas em processos de verificação de identidade⁴⁷. **Em nível regional**, a plataforma de banco digital Bankingly expôs os dados pessoais e financeiros de mais de 135 mil clientes de cooperativas e entidades microfinanceiras em países como Bolívia, Costa Rica, Equador, El Salvador, México e República Dominicana, após utilizar *buckets* do Azure⁴⁸ sem medidas de segurança adequadas⁴⁹.

Outro conjunto relevante de incidentes esteve associado à **vulnerabilidade da cadeia de suprimentos digital**, na qual o vazamento não ocorre diretamente na organização principal, mas sim em fornecedores de tecnologia que têm acesso a sistemas. No **Peru**, a violação de dados de clientes do Interbank teve origem no uso indevido de credenciais que permitiram o acesso a servidores gerenciados por um provedor de monitoramento externo, evidenciando os riscos críticos decorrentes da terceirização⁵⁰.

44. Argentina, Brasil, Chile, Colômbia, Costa Rica, Equador, Honduras, México, Paraguai, Peru, Uruguai e Venezuela.

45. Google Cloud Storage: Serviço de armazenamento em nuvem do Google que permite salvar e acessar grandes volumes de dados usando os chamados buckets. Uma configuração incorreta de permissões pode fazer com que esses buckets se tornem públicos e exponham informações confidenciais sem autenticação.

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

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

48. Buckets do Azure: Espaços de armazenamento em nuvem da Microsoft usados para armazenar e gerenciar arquivos e dados. Se configurados incorretamente, podem permitir o acesso não autorizado a informações sensíveis.

49. El Testigo, “Una filtración de datos afecta a las instituciones financieras de América Latina, incluida República Dominicana”, El Testigo (4 dez. 2024). Disponível em: <https://eltestigo.com/una-filtracion-de-datos-afecta-a-las-instituciones-financieras-de-america-latina-incluido-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 (10 nov. 2024). Disponível em: <https://ojo-publico.com/5390/ciberdelincuencia-la-ruta-de-tras-del-robo-datos-interbank>

Um padrão semelhante foi observado na **Argentina** com o ataque cibernético a um provedor de serviços de mensagens SMS, responsável pelo envio de códigos de verificação (OTP, na sigla em inglês) e mensagens associadas à autenticação e recuperação de contas⁵¹. Ao comprometer essa via de mensagens por SMS, os atacantes conseguiram interceptar o tráfego de SMS em tempo real, incluindo códigos OTP. Isso facilitou o sequestro de contas por meio de processos de redefinição de senha e outros fluxos que dependem da verificação por SMS, reduzindo a eficácia do segundo fator quando este se baseia em mensagens de texto.

O monitoramento regional também identificou vazamentos resultantes do **uso abusivo de acessos legítimos** por meio de credenciais formalmente com autorização formal, sem ser possível determinar se as ações foram realizadas pelos titulares das contas ou por terceiros que obtiveram acesso a essas contas. No **Peru**, houve a exposição de imagens e dados pessoais armazenados nos bancos de dados da RENIEC⁵². O incidente foi atribuído ao uso indevido de acesso concedido ao Ministério do Interior⁵³.

De forma semelhante, no **Ecuador**, investigou-se o vazamento de dados do serviço de emergência ECU 911 para empresas funerárias. Isso permitiu que estas contatassem parentes de pessoas em situações críticas mesmo antes de uma morte ocorrer, levantando questões éticas e de proteção de dados em contextos de vulnerabilidade⁵⁴.

Uma série de incidentes particularmente preocupantes **afetou instituições públicas e serviços essenciais**, expondo informações de milhões de pessoas. No **Paraguai**, dois vazamentos massivos — um do Tribunal Superior Eleitoral, envolvendo mais de 7 milhões de pessoas, e outro de entidades financeiras públicas com mais de 17 mil registros — expuseram dados altamente sensíveis, incluindo filiação política, informações de emprego e salários de funcionários públicos⁵⁵.

No **Uruguai**, foram registrados diversos vazamentos que afetaram órgãos estatais, incluindo a exposição de quase 15 mil pedidos de visto — a maioria de migrantes e refugiados —, bancos de dados de atendimento ao cidadão com mais de 574 mil registros e mais de 13 mil credenciais de acesso a sistemas do Estado^{56 57 58}. Enquanto

51. Juan Brodersen, "Hackean un proveedor de mensajes de texto en Argentina y alertan sobre estafas: qué pasó y cómo protegerse", Clarín (30 mar. 2025). Disponível em: https://www.clarin.com/tecnologia/hackean-proveedor-mensajes-texto-argentina-alertan-estafas-paso-protegerse_0_XqOTd0Yj2B.html

52. Entidade estatal autônoma responsável pela gestão do banco de dados pessoal dos cidadãos peruanos.

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

55. TEDIC, "Filtraciones masivas en Paraguay: cuando nuestros datos quedan a la deriva", TEDIC (31 mar. 2025). Disponível em: <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 (27 mar. 2025). Disponível em: <https://www.infobae.com/america/america-latina/2025/03/27/filtracion-en-migraciones-de-uruguay-expuso-15-mil-solicitudes-de-visa-en-su-mayoria-cubanos-y-pakistanies/>

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

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

isso, em **Honduras**, investigações jornalísticas documentaram a circulação de dados do censo eleitoral e milhões de números de telefone em sites de venda ilegal⁵⁹.

Os vazamentos que afetaram setores como **saúde** e educação constituem um dos impactos mais graves do período analisado. Na **Argentina**, mais de 665 mil estudos médicos de pacientes tratados em clínicas e hospitais foram colocados à venda. Os dados variam de imagens de raio-X, ultrassonografias e tomografias computadorizadas a exames laboratoriais⁶⁰. Em **El Salvador**, foram vazados dados pessoais de quase um milhão de pessoas ligadas ao sistema de seguridade social, além de 50 GB de informações de instituições de ensino e 141 GB de empresas de cobrança de dívidas^{61 62 63}. No **Chile**, um ataque de ransomware contra uma universidade resultou na divulgação de 46 GB de dados, incluindo informações pessoais e financeiras de alunos e funcionários da universidade⁶⁴. No **México** e no **Brasil**, ataques a instituições públicas de ensino expuseram dados de milhares de estudantes, em muitos casos menores de 18 anos, agravando os riscos para crianças e adolescentes^{65 66}.

Em todos os incidentes, os dados registrados mostram que os vazamentos não terminam no momento inicial da exposição dos dados. Pelo contrário, geralmente são amplificados por meio de sua **circulação e monetização em fóruns da dark web**, onde as informações são vendidas ou divulgadas em massa. Durante o período analisado, por exemplo, foi documentada a venda de cerca de 250 mil registros bancários de pessoas no **Brasil** por valores equivalentes a poucos créditos dentro desses mercados⁶⁷, bem como a venda de credenciais de acesso a sistemas fiscais no **México** — incluindo chaves de assinatura eletrônica — de pelo menos 111 mil contribuintes⁶⁸.

59. Mario Sánchez, “Datos de hondureños, de venta en sitios web clandestinos”, La Prensa (3 jun. 2024). Disponível em: <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 (4 abr. 2025). Disponível em: https://www.clarin.com/tecnologia/hackean-proveedor-software-medico-argentina-venden-resultados-estudios-pacientes_0_HmJFyOZYib.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 (17 set. 2024). Disponível em: <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 (7 jan. 2025). Disponível em: <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 (3 abr. 2025). Disponível em: <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 (14 nov. 2024). Disponível em: <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 (8 abr. 2025). Disponível em: <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 (13 ago. 2024). Disponível em: <https://www.intercept.com.br/2024/08/13/governo-de-alagoas-despeja-dados-de-alunos-e-professores/>

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

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

Na **Argentina** e na **Venezuela**, foram oferecidas bases de dados com milhões de registros pessoais, acompanhadas de amostras parciais, conhecidas como *samples*, que permitem aos compradores verificar a autenticidade das informações antes de adquirir os dados completos^{69 70}.

Esse ecossistema de revenda **não se limita a fóruns especializados**. Observou-se também um aumento no comércio de dados pessoais para plataformas de uso cotidiano, particularmente o Telegram. A investigação *Identities à venda: O mercado ilegal latino-americano de compra e venda de dados pessoais no Telegram*, de Derechos Digitales⁷¹ documentou a atuação de grupos e canais nessa plataforma dedicados à compra e venda ilegal de dados pessoais em diversos países da América Latina, onde endereços, números de telefone, informações de saúde, filiação política e outros dados sensíveis circulam com facilidade e a baixo custo.

Os incidentes de violação de dados mostram como a exposição repetida de informações pessoais tende a se normalizar na região, instilando uma perigosa **ideia de inevitabilidade**. No entanto, por trás de cada banco de dados vazado não estão apenas registros técnicos, mas pessoas cujos direitos estão comprometidos. Esses impactos não são distribuídos de forma igualitária: mulheres, crianças e adolescentes, pessoas LGBTQIA+, defensores dos direitos humanos e comunidades historicamente vulneráveis enfrentam riscos agravados de assédio, fraude, violência digital e perseguição quando suas informações são expostas.

Em termos técnicos, a aplicação de medidas como o princípio do privilégio mínimo, a criptografia da informação, a rastreabilidade de acesso, a autenticação multifatorial e a revisão periódica dos dados armazenados e do período de armazenamento constituem não apenas uma boa prática, mas também uma obrigação organizacional. Diversas dessas medidas devem ser integradas desde o desenvolvimento dos sistemas, seguindo o princípio da privacidade desde a concepção, segundo o qual a proteção de dados não é um acréscimo posterior, mas uma consideração desde o início.

3.4. Desinformação nas eleições

A desinformação tornou-se uma ferramenta estratégica nos processos eleitorais na América Latina. Em contextos de polarização e informações urgentes, a circulação de conteúdo falso ou enganoso — em textos, imagens, vídeos ou áudios — busca mobilizar emoções para influenciar o voto, favorecer ou prejudicar candidaturas e corroer a confiança no processo eleitoral. O monitoramento dos processos eleitorais na região revela padrões que combinam **táticas tradicionais e inovações**

69. Daily Dark Web, “Massive Database Leak Reportedly Exposes 43 Million Records in Argentina”, Daily Dark Web (5 jan. 2025). Disponível em: <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] (30 abr. 2025). Disponível em: <https://x.com/vesinfiltro/status/1917532243846705173>

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

tecnológicas, transformando a mentira organizada em um componente estrutural da competição política. Durante esse período, ocorreram eleições no Brasil, Chile, Equador, México, Uruguai e Venezuela, com as tendências apresentadas abaixo.

Uma tática recorrente é **semear dúvidas sobre a integridade do processo eleitoral com base em “evidências” que aparentam ser técnicas** — capturas de tela, números, vídeos — mas que na verdade são mal interpretadas ou tiradas de contexto. Aqueles que espalham desinformação aproveitam-se da falta de conhecimento dos cidadãos sobre os procedimentos para apresentar incidentes menores ou erros humanos como se fossem prova de uma fraude orquestrada.

No **México**, por exemplo, viralizou a notícia de que havia “registros duplicados” no Programa de Resultados Eleitorais Preliminares (Prep)⁷² como suposta prova de fraude, apesar de se tratar de uma contagem preliminar e informativa, sujeita a erros de captura ou digitalização que são posteriormente corrigidos nas contagens oficiais⁷³. Narrativas semelhantes ocorreram no Equador, construídas a partir de “evidências” visuais enganosas: um vídeo foi divulgado alegando que a autoridade eleitoral estava distribuindo canetas cuja escrita poderia ser apagada para alterar os votos. No entanto, o material correspondia a um vídeo retirado de contexto, de outro país e de outro ano^{74 75}. No cenário pós-eleitoral, uma imagem que viralizou atribuiu à OEA a declaração de que os resultados não eram legais, apesar de uma declaração oficial validar o processo⁷⁶.

Mesmo interrupções momentâneas em sites institucionais — como as relatadas pelo Instituto Eleitoral da Cidade do **México** durante o dia e o atraso na atualização do site da Servel ⁷⁷ — no **Chile**, foram reinterpretadas como sinais de manipulação e usadas para semear dúvidas sobre a integridade do processo^{78 79}.

72. O Programa de Resultados Eleitorais Preliminares (Prep) é um sistema informatizado implementado pelas autoridades eleitorais que fornece os resultados preliminares de uma eleição na mesma noite do dia da eleição, com base na contagem rápida das folhas de apuração que chegam das seções eleitorais.

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

74. Giuliana M. Andrade, “Es falso que el CNE entrega esferas que se borran”, LupaMedia (8 abr. 2025). Disponível em: <https://lupa.com.ec/verificaciones/cne-esferas-borrrables-elecciones-2025/>

75. Redacción Vistazo, “Correísmo denuncia en Fiscalía al CNE por “bolígrafos con tinta borrrable” que habrían perjudicado a Luisa González”, Vistazo (29 maio 2025). Disponível em: <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 (21 abr. 2025). Disponível em: <https://lupa.com.ec/verificaciones/oea-reconoce-resultados-ecuador/>

77. O Serviço Eleitoral do Chile é um órgão autônomo do Estado, com status constitucional, responsável por organizar, administrar e supervisionar os processos eleitorais e plebiscitários.

78. Cristóbal Palacios, “Lentitud en publicación de resultados: Servel informa desfase en actualización en su sitio web”, La Tercera (28 out. 2024). Disponível em: <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 (4 jun. 2024). Disponível em: <https://verificado.com.mx/desinformaciones-que-marcaron-jornada-electoral/>

Em paralelo, um padrão persistente de **falsificação de identidade** surge através de contas e conteúdos que imitam veículos de comunicação para fazer com que um rumor pareça uma notícia confirmada. Na **Venezuela**, perfis do TikTok com estética jornalística espalham versões não verificadas como se fossem fatos, como a suposta prisão ou fuga do presidente do Conselho Nacional Eleitoral. A repetição em várias contas ampliou sua visibilidade, gerou confusão e foi então explorada para desacreditar a imprensa independente e reforçar narrativas pró-governo⁸⁰.

No **Ecuador**, o monitoramento identificou casos de falsificação de identidade por meio de peças fabricadas que replicavam logotipos e estilos gráficos de veículos de comunicação e instituições públicas para projetar legitimidade. Sob esse pretexto, mensagens destinadas a incitar medo ou indignação — por exemplo, a falsa associação entre migração e crime ou a oferta de bolsas de estudo inexistentes — foram disseminadas em formatos visuais concebidos para consumo rápido, seja por meio de publicidade paga ou capturas de tela criadas para se tornarem virais sem questionamentos⁸¹.

Seguindo essa mesma lógica, imagens falsas atribuídas a figuras políticas ou vídeos reutilizados fora de contexto circularam para estabelecer narrativas inexistentes ou irregularidades. Na **Venezuela**, circularam capturas de tela falsas mostrando María Corina Machado parabenizando uma tentativa de golpe na Bolívia⁸². No **México**, um vídeo de 2021 mostrando uma pessoa votando com uma arma foi reutilizado como se correspondesse à eleição de 2024⁸³. Em ambos os casos, a aparência de autenticidade foi suficiente para que o conteúdo se tornasse viral antes de qualquer verificação, aproveitando a imediatez do consumo nas redes.

O salto qualitativo na desinformação eleitoral ocorreu com a **massificação das ferramentas de inteligência artificial**, que permitem a criação de conteúdo hiper-realista a baixo custo e a uma velocidade antes impensável. Os *deepfakes* — manipulações de vídeo ou áudio que fazem parecer que uma pessoa disse ou fez algo que nunca aconteceu — tornaram-se especialmente eficazes porque transformam uma narrativa falsa em “prova” audiovisual fácil de compartilhar. Na **Venezuela**, por exemplo, circulou um *deepfake* no qual uma voz gerada por inteligência artificial foi sobreposta a um vídeo real da dirigente Delsa Solórzano para fazê-la dizer que o candidato Edmundo González “nunca venceu” as eleições⁸⁴.

80. Podcápsula Informativa, “Organizaciones internacionales reportan violaciones a los derechos humanos y digitales en Venezuela, mientras falsos noticieros en Tiktok posicionan rumores y facilitan propaganda oficialista”, Cazadores de Fake News (21 out. 2024). Disponível em: <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 (9 abr. 2025). Disponível em: <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 (12 jul. 2024). Disponível em: <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 (4 jun. 2024). Disponível em: <https://verificado.com.mx/desinformaciones-que-marcaron-jornada-electoral/>

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

Áudios apresentados como “vazamentos” do WhatsApp atribuídos a María Corina Machado também circularam, mas após verificação, descobriu-se que eram falsos e criados com inteligência artificial⁸⁵.

No **Brasil**, a desinformação adotou um viés de gênero explícito. Pelo menos cinco ataques *com deepfakes* contra candidatas foram documentados: imagens ou vídeos falsos em que o rosto de uma mulher é inserido em corpos nus para gerar conteúdo sexual⁸⁶. Este conteúdo busca degradar e intimidar, associando diretamente a desinformação à violência de gênero no âmbito político.

Ao mesmo tempo, os casos demonstram que **a desinformação frequentemente opera de forma coordenada em múltiplas plataformas**⁸⁷. No **Brasil**, um estudo sobre grupos políticos de extrema-direita durante a campanha municipal de 2024 constatou que 17% dos links compartilhados no WhatsApp continham desinformação, em comparação com 7% no Telegram⁸⁸. Na **Venezuela**, foram documentadas redes de contas que se citam mutuamente e fingem ser de oposição para amplificar narrativas no X e no TikTok, enquanto outras camadas da operação usam o Telegram para assédio coordenado⁸⁹. Essa lógica atingiu maior sofisticação no **Ecuador**, onde se adicionou a publicidade paga: empresas registradas nos Estados Unidos supostamente usaram produtos do Google para disseminar anúncios de desinformação contra candidatos⁹⁰.

3.5. Ataques direcionados

Os ataques direcionados consistem em ações deliberadas contra infraestruturas, sistemas ou serviços digitais específicos e caracterizam-se por não operarem “aleatoriamente”, mas sim por selecionarem alvos previamente identificados e implementarem ações destinadas a atingir um objetivo específico, como obter acesso, interromper serviços, extorquir ou cometer fraude. Esta seção descreve diferentes tipos de ataques direcionados identificados na região, como campanhas de phishing, sequestro de contas, fraude em aplicativos e ataques contra infraestrutura digital.

Embora essas técnicas sejam usadas em contextos diferentes, é importante observar que as mesmas ferramentas e vetores de ataque também podem ser usa-

85. Mardylid Castillo, “Falso audio de María Corina Machado en el que ofende a Delsa Solórzano”, Cotejo.info (4 jun. 2024). Disponível em: <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 (nov. 2024). Disponível em: <https://desinformante.com.br/wp-content/uploads/2024/11/AI-in-the-2024-brazilian-elections.pdf>

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

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

89. Podcápsula Informativa, “Infiltrar, robar datos, estigmatizar y atacar, la ofensiva informativa del gobierno de Maduro contra la oposición”, Cazadores de Fake News (26 ago. 2024). Disponível em: <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 (9 abr. 2025). Disponível em: <https://lupa.com.ec/explicativos/desinformacion-electoral-ecuador-2025/>

dos contra ativistas, jornalistas, defensores dos direitos humanos ou organizações da sociedade civil. Compreender como esses ataques funcionam nos permite avaliar os riscos enfrentados por diferentes atores no ambiente digital e os impactos que esses incidentes podem ter no cotidiano das pessoas e no funcionamento de instituições-chave.

A motivação econômica continua sendo um dos principais fatores que impulsionam os ataques na região. Os métodos se diversificaram e se tornaram mais sofisticados, como ilustra a **proliferação de cavalos de Troia bancários**⁹¹ projetados para o ambiente latino-americano. Infranus, detectado principalmente no **México**, é uma mutação de um spyware que se tornou⁹² um trojan bancário com uma capacidade específica: modificar a área de transferência da vítima para substituir silenciosamente o número da conta para a qual o dinheiro está sendo transferido, desviando os fundos para os criminosos⁹³. Na **Colômbia**, campanhas direcionadas a órgãos públicos e empresas utilizaram cavalos de Troia de administração remota distribuídos por meio de e-mails de phishing⁹⁴. E-mails altamente personalizados que se faziam passar por bancos e serviços de mensagens; ao abrir o anexo, era instalado um software capaz de registrar as teclas digitadas, capturar telas e roubar credenciais⁹⁵.

Outra tendência em expansão é **o empréstimo via aplicativo**, que combina engenharia social com⁹⁶ extorsão e se sustenta em condições de vulnerabilidade econômica. No **Ecuador**, o Centro para a Autonomia Digital (CAD)⁹⁷ descreve como essa modalidade cresce ao aproveitar a falta de emprego formal e de crédito. Esses aplicativos oferecem empréstimos rápidos por meio de processos de aprovação simplificados, mas, uma vez instalados, solicitam permissões invasivas — contatos, galeria, localização, câmera e registros de chamadas — que se tornam a base para coerção. Após a concessão do empréstimo, impõem taxas de juros exorbitantes e prazos impossíveis; qualquer atraso desencadeia ameaças, difamação por meio de contatos e, em alguns casos, intimidação através do uso de fotos pessoais ou íntimas e rastreamento de localização, chegando até mesmo à geração de “dívidas” adicionais não solicitadas⁹⁸.

91. Os trojans bancários são um tipo de malware que é instalado secretamente no dispositivo da vítima com o objetivo de roubar credenciais de login. Seu nome deriva da analogia com o cavalo de Troia, pois são apresentados como programas legítimos para enganar e conseguir sua instalação.

92. Spyware é um tipo de malware que se instala secretamente em um dispositivo para coletar informações sobre um usuário sem o seu conhecimento ou consentimento, como senhas, mensagens, localização ou atividade na tela, e enviá-las a terceiros.

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

94. O phishing é uma técnica enganosa usada para obter informações confidenciais (como credenciais de login ou dados bancários) por meio da personificação de uma entidade legítima ou pessoa de confiança. É realizado por meio de comunicações falsas, mas aparentemente oficiais, como e-mails, mensagens de texto (smishing) ou chamadas telefônicas (vishing), que direcionam a vítima para sites fraudulentos criados para roubar seus dados ou infectar seu dispositivo com malware.

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

96. A engenharia social é o conjunto de técnicas de manipulação utilizadas para enganar pessoas e levá-las a revelar informações confidenciais, realizar ações específicas ou conceder acesso a sistemas protegidos. Ao contrário dos ataques puramente técnicos, a engenharia social explora a confiança, o medo, a curiosidade ou a falta de conhecimento.

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

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

No **México**, o Conselho Cidadão relatou mais de mil aplicativos desse tipo até 2024, vários dos quais estavam ativos no Google Play⁹⁹. No **Peru**, a Superintendência de Bancos e Seguros alertou sobre pelo menos 17 aplicativos com o mesmo esquema¹⁰⁰.

Por outro lado, a **falsificação de identidade** tornou-se um elo crucial na cadeia de fraudes digitais. O phishing continua sendo um dos vetores mais frequentes. Em **Honduras**, organizações indígenas e de defesa da terra têm sido alvo de campanhas de phishing personalizadas que se fazem passar por doadores internacionais para obter agendas de trabalho e mapear redes de contato, com o objetivo de facilitar a perseguição física por atores não estatais e empresas extrativistas¹⁰¹.

Esse mesmo vetor é usado para fins de fraude econômica: no **Chile**, mensagens sobre o vencimento de pontos em um popular programa de fidelidade do setor de combustíveis direcionavam para um site quase idêntico ao oficial, que solicitava dados bancários para um suposto custo de envio¹⁰². Na **Colômbia**, um esquema semelhante se fez passar pela Direção Nacional de Impostos e Alfândegas (DIAN) com notificações de dívida falsas¹⁰³. Esse tipo de engano é reforçado pelo uso da IA, que permite a produção de mensagens mais personalizadas e convincentes, reduzindo a eficácia dos sinais tradicionais de detecção.

Quando o golpe consegue obter credenciais, o roubo de contas torna-se uma ferramenta para intensificar a fraude. Na **República Dominicana**, a lista de vítimas inclui o presidente Luis Abinader, cujo perfil no Google X foi comprometido, além de ministros e o presidente do Senado; em diferentes casos, os atacantes usaram as contas para solicitar dinheiro de contatos, aproveitando-se da confiança associada à identidade falsificada¹⁰⁴. Em **Honduras**, uma quadrilha usou golpes de phishing para acessar contas do WhatsApp e, em seguida, ofereceu dólares a preços baixos; as vítimas transferiram o dinheiro para contas controladas pelos golpistas¹⁰⁵.

Uma técnica mais complexa é a *troca de SIM [SIM swapping]*, que explora a vulnerabilidade da verificação por SMS para se passar por uma pessoa junto à sua operadora de telefonia e transferir seu número para um cartão SIM controlado pelo atacante, obtendo assim acesso aos códigos de verificação que protegem contas

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 (28 jan. 2025). Disponível em: <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 (22 ago. 2024). Disponível em: <https://www.sbs.gob.pe/>

101. Fundación Acceso, “Observatorio Centroamericano de Seguridad Digital: Informe interanual 2020-2025 [Manuscrito no prelo].”

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

bancárias e outros serviços. No **Brasil**, uma organização criminosa ativou mais de 180 chips de celular com dados de terceiros para transferir a titularidade de linhas telefônicas, acessar contas bancárias e realizar transferências fraudulentas¹⁰⁶. Na **Costa Rica**, foi estabelecido um precedente legal: a Superintendência de Telecomunicações ordenou que a Claro indenizasse um cliente vítima de *troca de SIM*, constatando que a operadora não cumpriu sua obrigação de verificar a identidade da pessoa que solicitou a substituição do chip¹⁰⁷. A resolução coloca no centro do debate a responsabilidade das empresas de telefonia na proteção de seus clientes, além da mera prestação do serviço.

Ao mesmo tempo, uma onda de incidentes atingiu **instituições governamentais e serviços essenciais**, enfraquecendo a capacidade do Estado de prestar cuidados e manter as operações. O *ransomware*¹⁰⁸ consolidou-se como uma ameaça central nesta área. No **Uruguai**, hackers criptografaram as informações do governo departamental — incluindo backups — e exigiram 650 mil dólares em bitcoin, tornando os serviços digitais inoperantes e forçando processos de reconstrução¹⁰⁹. No **Paraguai**, o Ministério da Educação e Cultura sofreu um ataque que deixou todos os seus sites e procedimentos eletrônicos offline, e os atacantes exigiram um milhão de dólares¹¹⁰. Na **Argentina**, uma empresa responsável pela distribuição de cartões de crédito e documentos oficiais foi afetada por *um ataque de ransomware*, com risco de exposição de dados pessoais¹¹¹.

Houve também **incidentes com dimensões políticas**. Na **Bolívia**, a Agência de Governo Eletrônico registrou centenas de ataques contra sites estatais no final de 2024, e um dos episódios mais notórios comprometeu o site da Câmara do Senado, cuja página inicial foi substituída por mensagens e símbolos — um ataque conhecido como *desfiguração*^{112 113}. No **Brasil**, no mesmo dia em que o juiz Alexandre de Moraes ordenou o bloqueio do X, o Supremo Tribunal Federal e outras instituições estatais sofreram ataques cibernéticos simultâneos¹¹⁴. O momento em que ocorre-

106. Assessoria de Comunicação – PCDF, “PCDF desarticula organização criminosa especializada no golpe do Sim Swap”, Polícia Civil do Distrito Federal (12 fev. 2025). Disponível apenas no Brasil ou via VPN com servidor localizado no Brasil: <https://www.pcdf.df.gov.br/noticias/13572/pcdf-desarticula-organizacao-criminosa-especializada-no-golpe-do-sim-swap>

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

108. O ransomware é um tipo de malware que bloqueia o acesso a um sistema informático ou criptografia de arquivos da vítima, exigindo o pagamento de um resgate (geralmente em criptomoedas) em troca da sua liberação. Uma vez infectado, o dispositivo exibe uma mensagem na tela com instruções para efetuar o pagamento, geralmente acompanhada de uma contagem regressiva que aumenta a pressão sobre a vítima.

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

112. A desfiguração é um tipo de ataque que envolve o acesso não autorizado a um site e a modificação de seu conteúdo visível, substituindo a página principal por imagens e/ou mensagens escolhidas pelo atacante.

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

ram e o fato de os ataques também terem como alvo a agência responsável pela implementação do bloqueio sugerem uma ação coordenada em resposta à decisão judicial. Na **Costa Rica**, o acesso não autorizado a uma conta de e-mail institucional da Universidade da Costa Rica permitiu o envio de uma ameaça de bomba, forçando a evacuação do campus¹¹⁵.

Os ataques direcionados na região demonstram que os principais alvos são instituições públicas e empresas que lidam com informações sensíveis ou serviços essenciais; portanto, elas também detêm uma responsabilidade central em questões de segurança digital. Quando infraestruturas críticas ou sistemas de gestão de dados falham, os riscos não se limitam a fraudes financeiras, mas podem afetar a segurança das pessoas, o acesso a serviços e a capacidade dos cidadãos — incluindo jornalistas, ativistas e organizações sociais — de participar na vida pública. Em contextos em que organizações sociais e defensores dos direitos humanos dependem dessas plataformas para acessar informações públicas ou registrar denúncias, a interrupção dos serviços também pode obstaculizar os processos de prestação de contas e o acesso a direitos.

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

4. Áreas temáticas



4 Áreas temáticas

Esta seção consiste em uma sistematização das informações coletadas de diferentes fontes e níveis de evidência. Por um lado, integra informações obtidas a partir de dados e documentação de casos; por outro, incorpora experiências compartilhadas pelas organizações que integram o OLAD, bem como padrões e preocupações comuns identificados ao longo do trabalho conjunto do Observatório durante o período abrangido por este relatório.

Este capítulo se debruça sobre quatro áreas temáticas que emergiram com particular força na conversa regional e nos materiais analisados: a violência de gênero facilitada por tecnologias, a exploração de dados biométricos, os cortes de internet e a vigilância.

Ao longo das páginas seguintes, a análise combina evidências quantitativas com conhecimento situado das organizações, oferecendo uma visão panorâmica, porém detalhada, de como essas ameaças se manifestam na vida das pessoas e comunidades que defendem os direitos na América Latina.

4.1. Violência de gênero facilitada pela tecnologia

A Violência de Gênero Facilitada pela Tecnologia (VGFT) é uma das ameaças mais persistentes e em constante evolução na América Latina. Longe de serem incidentes isolados, fazem parte de uma rede de mecanismos que agressores — individuais ou coletivos — utilizam para assediar, controlar, humilhar, sexualizar, extorquir ou prejudicar mulheres e pessoas LGBTQIA+ por motivos relacionados ao seu gênero ou identidade, utilizando plataformas, dispositivos, sistemas algorítmicos e dados pessoais.

Durante o período abrangido por este relatório, as organizações do OLAD documentaram tanto a persistência de formas conhecidas de agressão quanto o surgimento de novas modalidades, o que demonstra a capacidade dos agressores de se adaptarem às tecnologias recentes e aos contextos sociopolíticos de cada país. A expansão das ferramentas de IA e os casos que ganharam visibilidade pública em diferentes países confirmam que essa violência não é uma soma de incidentes, mas um fenômeno estrutural que se reinscreve em novas infraestruturas técnicas e cenários sociais.

Organizações que operam linhas de apoio para vítimas de VGFT na região — como o Centro SOS Digital da Fundación InternetBolivia.org na **Bolívia** e Navegando Libres do Taller de Comunicación Mujer [Oficina de Comunicação Mulher] no **Equador** foram fundamentais para tornar visíveis as dinâmicas desse tipo de violência e, sobretudo, para fornecer apoio direto às pessoas afetadas¹¹⁶.

4.1.1. Navegando Libres

No caso da linha de ajuda **Navegando Libres**, os casos no Equador demonstram a persistência de formas conhecidas de VGFT¹¹⁷. É o caso de extorsão sexual, difamação, divulgação de conteúdo íntimo, assédio, falsificação de identidade e acesso não autorizado a contas. Muitos desses casos estão ligados a separações, conflitos familiares ou represálias contra mulheres com ativismo feminista e social.

Juntamente com essas manifestações recorrentes, a organização identificou formas emergentes particularmente graves. Uma delas é a violência facilitada por aplicativos de empréstimo: em um caso documentado, uma mulher que solicitou um empréstimo por meio de um aplicativo foi vítima de acesso não autorizado aos seus contatos sem o seu conhecimento e, quando os pagamentos atrasaram, tanto ela quanto sua família receberam ameaças, mensagens intimidatórias e fotomontagens com conteúdo humilhante.

Para a organização, esse fenômeno deve ser compreendido no contexto da precariedade econômica que afeta desproporcionalmente as mulheres no Equador, que enfrentam maior desemprego e maiores encargos familiares e de cuidado, além da desigualdade digital de gênero que limita seu conhecimento sobre o funcionamento desse tipo de aplicativo e as práticas de segurança digital.

Foram também relatados diversos casos em que os agressores usaram referências a gangues criminosas para aumentar o medo em situações de extorsão sexual,

116. Para saber mais sobre o trabalho dessas organizações no combate à violência de gênero facilitada pela tecnologia, consulte os recursos disponíveis em: <https://tcmujer.org/> e <https://internetbolivia.org/>

117. Para obter mais detalhes sobre o conceito e as formas de manifestação da VGFT de acordo com os padrões internacionais de direitos humanos, consulte: Derechos Digitales, *Combatir la violencia de género facilitada por tecnologías (VGFT) desde el enfoque del derecho internacional de los derechos humanos*. Disponível em: <https://www.derechos-digitales.org/recursos/combater-la-violencia-de-genero-facilitada-por-tecnologias-vgft-desde-el-enfoque-del-derecho-internacional-de-los-derechos-humanos/>

bem como ameaças de ex-parceiros com ligações a empresas de segurança do Estado, revelando como a VGFT está intrinsecamente ligada às estruturas de poder e ao acesso privilegiado às tecnologias de vigilância.

Ao acompanhar uma coletiva feminista, também foi documentado um caso de disseminação em massa de conteúdo íntimo em grupos do Telegram. Integrantes da coletiva tentaram se infiltrar e conseguiram identificar que uma das etapas para pertencer a esses grupos era compartilhar conteúdo sexual de parentes ou conhecidas do sexo feminino. Na sequência dessa exigência, existiam outros mecanismos de verificação aos quais não tinham acesso por razões de segurança, o que sugere uma estrutura organizada e hierárquica para a disseminação desse tipo de violência.

O trabalho de documentação e suporte também é afetado pelas decisões tomadas pelas plataformas. A suspensão temporária da conta do Instagram de Navegando Libres — que a organização atribui a mudanças nas políticas da Meta¹¹⁸ — evidencia como as plataformas podem enfraquecer, por ação ou omissão, infraestruturas de apoio essenciais para aqueles que sofrem violência digital.

4.1.2. S.O.S. Digital

Da mesma forma, as evidências quantitativas do **Centro SOS Digital** da Fundación InternetBolívia.org reforçam essa leitura regional e permite observar a magnitude do problema em outra escala. A linha de apoio registrou 377 casos de violência digital durante o período. O abuso sexual por meio das TIC (29,5%) e o assédio (21%) foram as formas de violência mais recorrentes, representando juntas quase metade dos casos.

Juntamente com estas, outras manifestações de violência também aparecem consistentemente, como difamação (10,5%), quebra de segurança (10%), abuso de informação (9,5%), ameaças (9,5%) e fraude (7%). Isso demonstra que a VGFT não se limita a um único repertório de agressão, mas geralmente é empregada por meio de múltiplas formas combinadas.

Os casos também mostram que as mulheres continuam sendo as mais afetadas e que a maior concentração de casos está na faixa etária de 25 a 54 anos, seguida pela faixa de 18 a 24 anos e, em menor grau, por adolescentes de 13 a 17 anos. Esse padrão sugere que, embora a violência digital afete diferentes faixas etárias, ela tem um impacto particularmente forte em mulheres jovens e adultas em estágios de alta exposição social, profissional, emocional e comunitária.

118. Ao longo de 2025, a Meta implementou modificações em suas políticas de moderação que afetaram particularmente o conteúdo relacionado a gênero, diversidade sexual e educação sexual, resultando em suspensões e restrições a contas pertencentes a organizações feministas e de direitos humanos em diversos países da região.

Outro elemento relevante é que a resposta da linha de apoio não se limita a uma dimensão técnica. Ao longo do período, as ações mais frequentes foram o apoio emocional, a orientação jurídica e a orientação tecnológica, sendo que a primeira teve um peso ligeiramente maior. Esses dados são importantes porque mostram que a VGFT produz danos que não podem ser resolvidos apenas por meio de aspectos técnicos de segurança digital ou gerenciamento de plataformas; também exigem respostas legais e apoio contínuo.

4.1.3. Outros casos

Para além do trabalho das organizações OLAD, foram identificados casos de VGFT em fontes públicas de diferentes países. A primeira é a circulação e amplificação de discursos misóginos em plataformas digitais, frequentemente impulsionada por dinâmicas algorítmicas. No **Brasil**, uma pesquisa realizada pela Núcleo e AzMina mostrou como o TikTok expõe progressivamente adolescentes do sexo masculino a conteúdos e narrativas de extrema-direita que degradam as mulheres¹¹⁹. No mesmo país, o Brasil Paralelo lançou uma campanha publicitária massiva contra o aborto na Meta, que combina segmentação, apelos emocionais e uma agenda ultraconservadora, abordando também questões de gênero e diversidade sexual¹²⁰.

Um segundo padrão é a persistência da violência sexual digital como mecanismo de coerção, humilhação ou chantagem. Essa lógica aparece nos casos de extorsão sexual relatados em aplicativos de namoro no **México**, onde os agressores constroem uma relação inicial de confiança e depois ameaçam divulgar imagens íntimas e obter dinheiro¹²¹. Isso também foi observado no **Ecuador**, no caso de um homem acusado de contatar uma adolescente via WhatsApp para solicitar arquivos de conteúdo sexual, após intensificar progressivamente o tom das mensagens¹²².

Um terceiro padrão, particularmente preocupante, é o uso da IA para sexualizar, desacreditar ou expor mulheres sem o seu consentimento. Na **Bolívia**, os ataques contra mulheres na política incluíram humilhação corporal, insinuações sexuais e *deepfakes* com o intuito de minar sua legitimidade pública¹²³. No **México**, essa mesma dinâmica afetou figuras públicas como uma senadora e uma streamer, por meio da disseminação de *deepfakes* de conteúdo sexual sem o seu consentimen-

119. Flávia Santos y Sofia Schurig, “Como o TikTok alimenta a misoginia entre adolescentes brasileiros”, Núcleo Jornalismo (3 abr. 2025). Disponível em: <https://nucleo.jor.br/reportagem/2025-04-03-tiktok-misoginiadeadolescentes/>

120. Paulo Motoryn, “Brasil Paralelo já gastou meio milhão de reais em anúncios contra aborto”, Intercept Brasil (21 jun. 2024). Disponível em: <https://www.intercept.com.br/2024/06/21/brasil-paralelo-ja-gastou-meio-milao-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 (12 fev. 2025). Disponível em: <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 (6 nov. 2024). Disponível em: <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 (25 abr. 2025). Disponível em: <https://boliviaverifica.bo/insultos-montajes-y-amenazas-la-guerra-silenciosa-contra-las-mujeres-en-la-politica-boliviana/>

to^{124 125}. E no **Chile**, um estudante foi acusado de criar *deepfakes* de cunho sexual de suas colegas de classe, o que demonstra o quanto essas ferramentas já estão disponíveis e podem ser usadas para causar danos sem a necessidade de conhecimento técnico avançado¹²⁶.

Este último padrão está diretamente relacionado com as conclusões de **uma investigação sobre aplicativos deepfake na América Latina**. Com base na coleta automatizada de dados no Google Play, foram identificados 105 aplicativos disponíveis em dezembro de 2024. O estudo concluiu que 89,5% desses aplicativos representam um perigo potencial para as mulheres¹²⁷.

Os resultados mostram que essas ferramentas não são difíceis de encontrar ou usar. Pelo contrário, plataformas como o Google Play legitimam esse ecossistema ao permitirem a circulação em massa de tecnologias que facilitam a agressão simbólica e sexual sem consentimento, sob esquemas comerciais lucrativos. A isso se soma a facilidade de uso, a presença de imagens promocionais sexualizadas, classificações etárias enganosas e uma falta generalizada de transparência quanto à origem de muitos desses aplicativos. Esse ecossistema é resultado de decisões empresariais que priorizam o lucro em detrimento da segurança de mulheres e pessoas LGBTQIA+, e que tornam as plataformas cúmplices da violência de gênero.

4.2. Exploração de dados biométricos

A exploração de dados se refere a contextos em que as informações pessoais das pessoas, especialmente quando se trata de dados sensíveis, deixam de ser apenas dados sobre elas e se tornam um recurso do qual outros obtêm benefícios econômicos ou estratégicos. Não se trata apenas de uma empresa coletar informações, mas de questionar em que condições isso ocorre, o que ela obtém em troca, o quanto as pessoas entendem sobre esse processamento e se elas mantêm alguma liberdade para decidir ou, posteriormente, recuperar o controle sobre seus dados.

Quando dados biométricos estão em jogo, o problema assume uma dimensão ainda mais delicada. Ao contrário de uma senha, a íris, o rosto ou as impressões

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

125. Ignacio Izquierdo, “Alana Flores es víctima del ‘deepfake’ y anuncia acciones legales contra usuario”, *Infobae*, 27 maio 2025. Disponível em: <https://www.infobae.com/mexico/2025/05/27/alana-flores-es-victima-del-deep-fake-y-anuncia-acciones-legales-contra-usuario/>

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

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

digitais não podem ser alterados se forem comprometidos, e o tratamento a eles realizado pode ter efeitos duradouros.

O caso da World, anteriormente Worldcoin, nos permite observar esse problema. Para compreender as respostas institucionais descritas abaixo, é necessário voltar brevemente ao que aconteceu em 2023. A partir daquele ano, longas filas começaram a se formar em diversas cidades da Argentina em frente a aparelhos que escaneavam a íris das pessoas que se aproximavam. Em troca, a empresa ofereceu o equivalente a entre 30 e 50 dólares em criptomoedas¹²⁸. Em agosto daquele ano, 9.500 argentinos registraram suas íris em um único dia (uma pessoa a cada nove segundos), em meio a uma inflação superior a 115% ao ano¹²⁹.

O fenômeno se repetiu em outros países da região com economias sob pressão, como Equador, Chile, Peru, Colômbia e República Dominicana¹³⁰. Atrás dessas fileiras estava a Worldcoin, um projeto cofundado por Sam Altman, também fundador da OpenAI¹³¹, cuja implementação na América Latina foi confiada à empresa Tools for Humanity (TFH). O projeto oferece uma identidade digital baseada na leitura da íris, com a promessa de criar um sistema global capaz de distinguir humanos de bots na internet. Com base nesse caso, esta seção examina como os dados biométricos podem se tornar uma fonte de valor para as empresas e por que isso gerou preocupações entre autoridades, tribunais e organizações da sociedade civil.

O World funciona a partir de dois momentos: o registro e o uso posterior da identidade digital. Durante o cadastro, a pessoa baixa o aplicativo World App e fornece dados como nome, número de telefone, endereço de e-mail, conta bancária e metadados do dispositivo. Em seguida, você deve comparecer pessoalmente a um dispositivo chamado *Orb*, que escaneia sua íris para concluir a verificação. A partir dessas imagens, o sistema gera um código de íris — uma representação numérica da textura da íris — e o compara com códigos anteriores para verificar se a pessoa já se cadastrou antes. Se o código for único, uma credencial digital chamada *World ID* será criada¹³².

A empresa afirma que não preserva a imagem da íris como uma fotografia, mas sim a transforma em códigos e fragmentos¹³³ para reduzir sua exposição direta. No entanto, isso não elimina o problema de fundo: mesmo que a imagem não seja divulgada como uma fotografia, a biometria continua sendo a base do sistema, pois a

128. York Perry, “Worldcoin bate récord en Argentina pese a los riesgos y 9.500 personas se registran en un día”, FayerWayer (5 set. 2023). Disponível em: <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 (31 ago. 2023). Disponível em: <https://www.diariobitcoin.com/argentina/worldcoin-record-argentina-9-500-registros-dia/>

130. Pedro Martín Sánchez, “El caso de Worldcoin y la alerta de las autoridades con criptomonedas”, Diario Libre (16 nov. 2024). Disponível em: <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”, Wikipedia, la enciclopedia libre (11 abr. 2026). Disponível em: <https://es.wikipedia.org/w/index.php?title=Worldcoin&oldid=172924752>

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

133. Esses códigos são conhecidos como IrisCode, representações binárias geradas a partir dos padrões únicos da íris usando um algoritmo de codificação. Ao contrário de uma senha, esse código não pode ser modificado se for comprometido, pois deriva diretamente de uma característica física imutável.

verificação da unicidade depende dela. Os dados mudam de forma, mas continuam sendo essenciais¹³⁴.

Após a conclusão do cadastro, o uso do World ID não exigirá mais uma nova digitalização. Segundo a empresa, o sistema utiliza ferramentas criptográficas para que a pessoa possa comprovar que pertence ao grupo de pessoas verificadas sem revelar novamente seus dados biométricos ou sua identidade civil. A promessa do projeto é precisamente essa: permitir que alguém prove ser um “ser humano único” em diferentes serviços digitais sem expor novamente os dados biométricos originais¹³⁵.

Para reforçar essa promessa de privacidade, eles incorporam mecanismos como fragmentação de dados, computação multipartidária segura e provas de conhecimento zero (SMPC e ZKPs, respectivamente). Em termos simples, essas técnicas visam garantir que nenhuma parte do sistema tenha acesso completo ao código da íris e que certas verificações possam ser realizadas sem revelar todas as informações subjacentes.

Essa arquitetura técnica, no entanto, não elimina as tensões de fundo. Um dos fatores é o consentimento: em diversos países, o cadastro foi promovido por meio de incentivos econômicos, o que complica a ideia de uma decisão totalmente livre, especialmente quando os cadastrados eram, em sua maioria, pessoas em situação econômica precária, dispostas a entregar dados insubstituíveis em troca de alguns dólares em criptomoedas. A questão não é apenas se a pessoa concordou, mas em que condições o fez e o quanto realmente compreendeu sobre o processamento de seus dados biométricos.

Outra tensão tem a ver com o risco a longo prazo. Mesmo quando a empresa promete anonimização ou fragmentação, permanecem dúvidas sobre o que realmente significa excluir dados biométricos depois de terem sido capturados, transformados e vinculados a uma credencial digital. A isso se soma um risco adicional decorrente da complexidade do próprio sistema. Uma auditoria técnica realizada em março de 2025 identificou múltiplas vulnerabilidades nos circuitos criptográficos do World, incluindo falhas que poderiam permitir que um invasor se registrasse várias vezes, burlando o mecanismo de unicidade¹³⁶. Embora a empresa tenha resolvido os problemas mais graves, a auditoria também alertou para riscos estatísticos não resolvidos. A existência dessas lacunas reforça as preocupações com a segurança de um sistema que lida com dados insubstituíveis.

Permanece também a questão de quem realmente controla esses dados e para quais fins. A promessa de que os dados “não são usados para outros fins” depende fortemente de alegações corporativas e mecanismos técnicos difíceis de auditar de forma independente.

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 (23 jan. 2025).

135. Ibid.

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

Essas tensões não permaneceram apenas no nível conceitual. Em diversos países da região, a implementação do World desencadeou respostas institucionais que permitem uma observação mais precisa dos problemas do modelo. No **Brasil**, a Autoridade Nacional de Proteção de Dados (ANPD) abriu uma investigação formal sobre o tratamento de dados biométricos pela World Foundation e pela TFH. A investigação teve como foco a coleta em larga escala de dados sensíveis e na forma como a empresa obteve o consentimento. A principal preocupação era que o cadastro fosse promovido por meio de compensação financeira em criptomoedas, o que poderia comprometer a liberdade de consentimento, especialmente porque envolvia dados sensíveis e difíceis de reverter. Em janeiro de 2025, a ANPD ordenou a suspensão da compensação financeira oferecida e também exigiu medidas de transparência, como a nomeação de um encarregado de proteção de dados pessoais.

A empresa tentou modificar seu modelo com um esquema de convites, onde a recompensa não estava mais vinculada à digitalização em si, mas à entrada de novas pessoas. Mas as autoridades consideraram que os riscos persistiam e mantiveram as restrições, mesmo com a possibilidade de multas diárias.

No **Chile**, durante 2024, o Serviço Nacional do Consumidor (SERNAC)¹³⁷ questionou a falta de informações claras sobre as finalidades do processamento, os riscos associados e as entidades que poderiam ter acesso aos dados, direcionando a discussão para os direitos do consumidor. Pouco tempo depois, a Suprema Corte aceitou um recurso de proteção apresentado pela mãe de um adolescente cuja íris foi escaneada¹³⁸. O tribunal ordenou a remoção do documento de identidade mundial do menor e de todos os registros de seus dados biométricos, ressaltando que, como ele tinha menos de 18 anos, não havia consentimento válido de seus representantes legais. A decisão foi clara, pois a empresa não deveria ter coletado esses dados sem verificar a idade e sem o consentimento correspondente.

A este cenário se soma a pesquisa da Fundação Amaranta, que oferece uma perspectiva contextualizada e de gênero¹³⁹. Com base em entrevistas, o estudo mostra que aqueles que entregaram suas digitalizações de íris eram, em sua maioria, mulheres-mães com necessidades econômicas urgentes. Revela também que, em muitos casos, as pessoas não entendiam o que a empresa fazia com seus dados, quais riscos esse processamento acarretava ou quão possível era excluir essas informações posteriormente. O estudo confirma que o problema está intrinsecamente ligado a contextos de precariedade, desigualdades de gênero e assimetrias de informação que enfraquecem a possibilidade de uma decisão realmente livre.

Além do Brasil e do Chile, o caso World também gerou alertas em outros países da região. No **Peru**, a empresa foi investigada pela ANPD em meio a um debate

137. É o órgão público chileno responsável por proteger e promover os direitos dos consumidores, monitorar o cumprimento das normas e poder iniciar ações judiciais em defesa de seus interesses.

138. SERNAC, “SERNAC denuncia ante la Justicia a Worldcoin por recolección indebida de datos biométricos”, Servicio Nacional del Consumidor (28 ago. 2024). Disponível em: <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 (2 jan. 2025). Disponível em: <https://amarantas.org/wp-content/uploads/2025/01/ong-amaranta-datos-biometricos.pdf>

público sobre a segurança dos dados biométricos e a legalidade do modelo de escaneamento da íris em troca de criptomoedas^{140 141}. Na **República Dominicana**, Pro Consumidor ordenou a suspensão das atividades após detectar possíveis cláusulas abusivas em contratos e problemas relacionados ao dever de informação, à ausência de um escritório registrado local e ao tratamento de dados biométricos em troca de um benefício econômico¹⁴². No **Ecuador**, a implementação do projeto também foi rodeada por questionamentos públicos e fechamentos devido à falta de licenças, em um contexto no qual organizações e especialistas alertavam para a falta de transparência das empresas aliadas e a fragilidade institucional para supervisionar efetivamente esse tipo de prática¹⁴³.

O que esses casos demonstram é que, apesar de sua sofisticação técnica, o modelo mundial deixa em aberto questões centrais sobre a validade do consentimento, o controle efetivo dos dados, a jurisdição aplicável e os riscos associados a uma possível violação de informações biométricas. Por trás de cada íris escaneada, há uma pessoa que jamais poderia ter imaginado as consequências daquela troca de informações.

4.3. Bloqueios de internet

Um corte de internet, também conhecido como apagão ou bloqueio da internet, é uma interrupção no funcionamento da conectividade que impede o acesso total ou parcial à rede em uma determinada área. Pode ser causada por fatores intencionais e acidentais e afetar áreas que variam de localidades específicas, como uma cidade, a regiões mais amplas, incluindo países inteiros. A duração desses eventos é variável e pode ir de minutos a vários dias, dependendo de sua origem e magnitude¹⁴⁴.

Diferentemente dos casos documentados no capítulo sobre censura, em que sites ou plataformas específicas são restringidas, os cortes afetam a própria conectividade. Suas consequências prejudicam o direito de buscar e disseminar informações, limitam a liberdade de expressão, dificultam o acesso a serviços básicos como saúde e educação e, em contextos de emergência, podem isolar comu-

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 (3 jun. 2024). Disponível em: <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 (3 jun. 2024). Disponível em: <https://www.gob.pe/institucion/anpd/noticias/965752-minjUSDH-supervisa-la-recopilacion-de-datos-personales-por-worldcoin>

142. Comunicaciones Pro Consumidor, “Pro Consumidor suspende las operaciones de Worldcoin en República Dominicana”, Pro Consumidor (15 nov. 2024). Disponível em: <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 (18 set. 2024). Disponível em: <https://labarraespaciadora.com/worldcoin-datos-biometricos/>

144. Coop La Lonja, “Corte De Internet: Ataque A La Libertad De Expresión”, Coop La Lonja (12 jan. 2012). Disponível em: <https://cooplalonja.com.ar/corte-de-internet/>

des inteiras em momentos em que elas mais precisam se comunicar.

As causas podem ser muito diferentes. Os **cortes intencionais** são aquelas em que um ator, geralmente estatal, interrompe (ou ordena a interrupção) deliberada da conectividade, geralmente para controlar o fluxo de informações durante protestos ou processos eleitorais. Os **cortes colaterais** ocorrem quando a internet cai como consequência de outro evento, como uma crise energética, sem que ninguém tenha ordenado diretamente, mas com o mesmo efeito prático sobre as pessoas. Um terceiro tipo inclui casos em que a desconexão responde a anos de **infraestrutura deteriorada**, sem que um evento específico a tenha causado.

Durante o período abrangido por este relatório, a América Latina registrou casos dos três tipos na Venezuela, Equador, Chile, Panamá, Cuba e Colômbia. A análise combina a documentação técnica de organizações do OLAD — incluindo a Conexión Segura, por meio de sua iniciativa de monitoramento **VE Sin Filtro** na Venezuela, e a Fundación Karisma, por meio do **Observatório de Bloqueio da Internet** (OBI) do K+Lab na Colômbia — com uma sistematização de casos públicos documentados pela mídia e por iniciativas globais de monitoramento.

Dentre os casos documentados de **cortes intencionais** na região, destaca-se o caso do **Panamá**. Em junho de 2025, o governo suspendeu o acesso à internet e à telefonia móvel na província de Bocas del Toro por quase duas semanas, em resposta às mobilizações sociais contra uma reforma do sistema de previdência social¹⁴⁵. A medida foi implementada no âmbito da declaração de estado de emergência.

Um ano antes, a VE Sin Filtro documentou uma interrupção de conectividade na **Venezuela** que afetou exclusivamente a CANTV e a Movilnt, as duas principais operadoras estatais, por quase duas horas, deixando vários estados sem sinal¹⁴⁶. Não houve explicação oficial e, embora não seja possível confirmar se foi intencional, o incidente ocorreu quatro dias após as eleições presidenciais de 28 de julho de 2024, em meio a uma escalada de bloqueios de sites. A falta de transparência oficial em torno desse incidente é, por si só, parte de um padrão.

Os impactos colaterais na região durante o período foram marcados principalmente por crises energéticas que prejudicaram a conectividade. O **Equador** foi o primeiro país a enfrentar esses problemas, já que uma seca severa afetou as usinas hidrelétricas, responsáveis por 72% da geração de eletricidade nacional¹⁴⁷. Isso provocou apagões que duraram até 14 horas por dia, deixando várias províncias sem internet durante meses¹⁴⁸. Na **Venezuela**, entretanto, um colapso no sistema elétrico nacional em 30 de agosto de 2024 deixou o país sem conecti-

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

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

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

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

dade por quase 21 horas, com 8 em cada 10 pessoas sem acesso à internet¹⁴⁹. O governo atribuiu o apagão à sabotagem da oposição, a mesma narrativa que seria repetida nos meses seguintes, sempre que o sistema elétrico entrava em colapso novamente¹⁵⁰.

Cuba registrou o maior número de incidentes durante o período. Entre outubro de 2024 e março de 2025, o país sofreu quatro colapsos no sistema elétrico nacional que afetaram a conectividade. A primeira, causada por uma falha na usina termoelétrica, deixou 10 milhões de pessoas sem eletricidade ou internet¹⁵¹. Os danos causados pelo furacão Rafael ocorreram em novembro¹⁵². Uma nova falha em dezembro e outra em março de 2025 decorrem da mesma causa: escassez de combustível e infraestrutura obsoleta sem manutenção¹⁵³. O **Chile** vivenciou seu próprio episódio quando uma falha massiva na rede elétrica deixou 14 das 16 regiões do país sem energia, interrompendo os serviços de internet e telefonia móvel por mais de 12 horas, no que foi o maior apagão desde 2010¹⁵⁴.

Na **Colômbia**, o OBI da Karisma documentou dois cortes na província de Chocó em agosto de 2024. O primeiro durou entre 6 e 12 horas¹⁵⁵ e coincidiu com uma tempestade torrencial que interrompeu o fornecimento de energia, e o segundo durou entre 3 e 6 horas¹⁵⁶. Esses casos também fazem parte de um contexto de precariedade em que apenas 13% da população tem acesso à internet, principalmente na capital do departamento, o que significa que qualquer interrupção afeta uma comunidade que já possui acesso muito limitado.

Um terceiro tipo de interrupção se manifesta como uma desconexão progressiva devido à deterioração da infraestrutura. Cuba ilustra claramente essa dinâmica, já que entre outubro e dezembro de 2024, o país ficou em último lugar no mundo em velocidade de download, com uma média de 2,96 Mbps, insuficiente até mesmo para tarefas básicas como videochamadas ou streaming de vídeo em qualidade padrão, que exigem pelo menos 10 Mbps¹⁵⁷. Em maio de 2025, a velocidade havia melhorado minimamente para 3,35 Mbps, permanecendo entre as mais baixas do

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

150. Wikipedia, “Apagones de Venezuela de 2024”, Wikipedia, la enciclopedia libre (22 fev. 2026). Disponível em: https://es.wikipedia.org/wiki/Apagones_de_Venezuela_de_2024

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

152. Diktyon y IODA, “Cuba enfrenta apagones y cortes de internet tras falla de la red eléctrica nacional”, IODA (27 nov. 2024). Disponível em: <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 (14 mar. 2025). Disponível em: <https://elpais.com/america/2025-03-15/un-nuevo-apagon-deja-a-cuba-a-oscuras-en-su-peor-crisis-energetica-en-decadas.html>

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

156. K+Lab, “[MICRO-CAIDA] Reporte: Caída de Red — Quibdó, Chocó 2”, Fundación Karisma (28 nov. Noviembre 2024). Disponível em: <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). Disponível em: https://github.com/diktyoncuba/public/blob/main/Informes/Informe-7_Oct-Dic-2024.pdf

índice global¹⁵⁸. Décadas de desinvestimento, agravadas por um bloqueio econômico que limitou o acesso à tecnologia e ao financiamento externo, e pela dependência de uma única empresa estatal, resultaram em uma infraestrutura obsoleta que não consegue manter a conectividade mínima para a população.

Além disso, os pacotes de internet ilimitada em pesos cubanos estão sendo restringidos para priorizar pagamentos em dólares estadunidenses pelos serviços prestados pela ETECSA¹⁵⁹. A partir de maio de 2025, serão introduzidos pacotes em moeda estrangeira e estabelecidos limites para gastos em moeda nacional¹⁶⁰. O resultado é que qualquer plano de dados além do limite básico ultrapassa o salário mínimo mensal do país, tornando a conectividade um privilégio econômico para aqueles sem acesso a moeda estrangeira¹⁶¹. Cuba não está desconectada tecnicamente, mas para quem não tem moeda estrangeira, a diferença prática para um apagão é mínima.

4.4. Vigilância

A vigilância digital consiste no monitoramento, interceptação, coleta e análise de dados on-line, realizados por agentes estatais ou privados, com o objetivo de controlar ou neutralizar indivíduos considerados de interesse¹⁶². Na América Latina, essa prática tem sido historicamente direcionada contra pessoas que defendem os direitos humanos, dando continuidade a práticas de vigilância presentes desde os períodos coloniais. O que durante décadas funcionou por meio de vigilância física ou escutas telefônicas agora é complementado — sem substituí-los — por novos métodos implementados nos dispositivos das pessoas, analisando seus rostos e monitorando suas palavras on-line, muitas vezes imperceptíveis para quem as observa, tornando-se ferramentas eficazes de controle e repressão.

A vigilância digital na América Latina manifestou-se através de diversas modalidades que refletem a expansão do controle estatal sobre a vida das pessoas na região. Entre as tendências documentadas estão o uso de *spyware* contra jornalistas e ativistas; o acesso físico forçado a dispositivos durante prisões ou operações policiais; a implantação de sistemas de reconhecimento facial, vigilância por vídeo em massa e plataformas de análise de dados massiva; e o patrulhamento cibernético em redes sociais.

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

159. Companhia Cubana de Telecomunicações SA (ETECSA)

160. Orlando González, "ETECSA aumentará as tarifas e dolarizará os serviços em 2025", Guardiões Digitais (2025). Disponível em: <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 (6 jun. 2025). Disponível em: <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). Disponível em: https://www.acceso.or.cr/wp-content/uploads/2021/08/2020_Art_Herramientas_Vigilancia_CA-mayo2020.pdf

Durante o período abrangido por este relatório, as organizações do OLAD documentaram esses fenômenos sob diferentes perspectivas. A **Fundación Acceso** investigou os efeitos psicossociais do *spyware* nas pessoas que sofreram com ele na América Central e documentou tendências críticas de vigilância por meio do Observatório Centro-Americano de Proteção Digital. Já **Conexión Segura** e sua iniciativa de monitoramento VE Sin Filtro registraram a implantação de tecnologias de vigilância na Venezuela durante o processo eleitoral de 2024. Essas contribuições são complementadas por casos documentados pela mídia, o que nos permite construir um panorama regional do fenômeno.

O uso de *spyware* acumulou novas evidências durante esse período. No **México**, documentos judiciais do processo entre o WhatsApp e a empresa israelense NSO Group — fabricante do *spyware* Pegasus — revelaram em abril de 2025 que 456 pessoas foram atacadas com esse software entre abril e maio de 2019, durante o governo de Andrés Manuel López Obrador, tornando o país com o maior número de vítimas, de um total de 1.233 identificadas globalmente¹⁶³. O Ministério da Defesa Nacional havia assinado um contrato para adquirir o Pegasus em abril daquele mesmo ano, e o operador final do sistema seria o Centro de Inteligência Militar, uma agência secreta cuja existência tem sido repetidamente negada pelas próprias forças armadas.

Em 2024, os Estados Unidos confirmaram que financiaram o uso do sistema Pegasus na **Colômbia** para operações de combate ao narcotráfico durante o governo de Iván Duque, pagando 11 milhões de dólares¹⁶⁴. Embora a versão oficial dos EUA afirmasse que Duque não foi informado, especialistas e uma denúncia criminal questionaram essa versão, apontando que um acordo dessa magnitude dificilmente poderia ter sido feito sem o conhecimento do Executivo^{165 166}.

No **Equador**, a Assembleia Nacional decidiu, em dezembro de 2024, iniciar um processo de supervisão após alegações de uso do Pegasus pelo governo de Daniel Noboa para monitorar jornalistas, membros da oposição e ativistas, embora, até o momento deste relatório, o processo não tenha apresentado resultados públicos¹⁶⁷.

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

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

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

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



Para além dos números, por trás de cada tecnologia de vigilância existem pessoas que sofrem as consequências. Um estudo da **Fundación Acceso**, publicado em abril de 2025, explorou, por meio de entrevistas com defensores dos direitos humanos e jornalistas da **América Central** infectados por *spyware*, os impactos concretos de terem sido submetidos a esse tipo de vigilância¹⁶⁸. As pessoas entrevistadas descreveram impactos que começaram com um pânico inicial e levaram a estados prolongados de alerta constante, ansiedade, insônia e depressão. Muitas pessoas mudaram seus trajetos, deixaram de frequentar certos lugares, modificaram seus hábitos nas redes sociais e migraram para aplicativos de mensagens mais seguros. Alguns até acabaram no exílio.

O impacto também se estendeu às equipes de trabalho, já que, quando uma pessoa revela que estava sendo vigiada, uma cadeia de pânico é desencadeada, forçando a alocação de tempo e recursos para a segurança em vez do trabalho de defesa. A isso se soma o impacto econômico, como a compra de novos aparelhos, despesas com terapia psicológica ou custos de mudança.

Nesse contexto, a Fundación Acceso desenvolveu um guia de apoio abrangente para pessoas que prestam serviços de proteção digital a indivíduos afetados por *spyware* e outras tecnologias de vigilância¹⁶⁹.

Com relação à América Central, o Observatório Centro-Americano de Proteção Digital¹⁷⁰, fomentado pela Fundación Acceso, registrou diversas tendências críticas entre 2024 e 2025¹⁷¹. Na **Guatemala** e na **Nicarágua**, o acesso físico aos dispositivos permitiu que promotores e governos construíssem narrativas de “conspiração” usando ferramentas criptografadas legítimas como supostas provas de criminalidade.

Especificamente, o governo de Daniel Ortega na **Nicarágua** consolidou uma infraestrutura que opera em múltiplas camadas. Desde 2017, opera em uma base militar em Manágua uma infraestrutura que combina radiogoniometria — capaz de localizar sinais telefônicos — com o sistema SORM-3, que permite a interceptação de chamadas, mensagens, e-mails, redes sociais e transações bancárias¹⁷².

168. Olga Paz, “Estudio de impactos y afrontamientos psicosociales ante ataques digitales”, Fundación Acceso (abr. 2025). Disponível em: https://pasalavoz.acceso.or.cr/Estudio_impactos_psicosociales_spyware_FAceso.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 (30 jul. 2025). Disponível em: <https://pasalavoz.acceso.or.cr/guia.htm>

170. Registro e análise sistemáticos de incidentes de segurança digital que afetam defensores dos direitos humanos, jornalistas e organizações da sociedade civil na América Central. Disponível em: <https://www.acceso.or.cr/observatorio-centroamericano-de-proteccion-digital/>

171. Fundación Acceso, “Observatorio Centroamericano de Seguridad Digital: Relatório Interanual 2020-2025 [Manuscrito em preparação]”.

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

A isso se soma a perseguição transnacional de exilados na **Costa Rica** por meio de *divulgação de informações pessoais* e monitoramento de mídias sociais¹⁷³.

Na **Venezuela**, a Conexión Segura documentou a utilização de diversas tecnologias de vigilância durante o processo eleitoral¹⁷⁴. Eles identificaram uma campanha de phishing direcionada a apoiadores da oposição, utilizando um formulário falso que coletava dados pessoais como endereço. O link malicioso foi divulgado por meio de contas falsas no X, Instagram, TikTok e Telegram. Além disso, o uso de drones para capturar imagens de manifestações, com foco nos rostos dos participantes, foi registrado e posteriormente divulgado por porta-vozes do governo.

Em paralelo, documentaram relatos de buscas ilegais em telefones celulares durante operações policiais, nas quais agentes exigiam o desbloqueio dos aparelhos para inspecionar conversas do WhatsApp e buscar termos associados a figuras políticas da oposição. A situação foi agravada pela instrumentalização do aplicativo estatal VenApp, originalmente criado para denunciar falhas em serviços públicos, que passou a ser usado para encaminhar denúncias anônimas ao governo contra manifestantes, por meio do envio de fotografias e dados de geolocalização, o que possibilitou localizar as pessoas denunciadas.

Esses métodos são complementados pela expansão das tecnologias de vigilância em espaços públicos, **como a vigilância por vídeo em massa e o reconhecimento facial**. No **Brasil**, São Paulo implementou o sistema Smart Sampa no final de 2024, uma iniciativa de videovigilância e reconhecimento facial com o objetivo declarado de identificar fugitivos e prevenir crimes, comparando imagens em tempo real com bancos de dados judiciais. Isso envolveu a instalação de 40 mil câmeras em espaços públicos e privados no âmbito municipal¹⁷⁵. Mais de 8% dos detidos pelo sistema Smart Sampa tiveram que ser liberados por engano: um aposentado de 80 anos ficou detido por horas porque o sistema o identificou como criminoso sexual; um paciente psiquiátrico foi algemado em um centro de saúde mental devido a um mandado de prisão desatualizado. Organizações da sociedade civil também apontaram que os dados oficiais não registram a identidade racial de mais da metade das pessoas detidas, o que impossibilita avaliar se o sistema pratica racismo algorítmico.

A expansão do sistema também atingiu ambientes educacionais, com quase 400 câmeras Smart Sampa instaladas em escolas municipais de São Paulo, onde o reconhecimento facial opera em áreas de acesso, gerando registros biométricos de alunos, professores e funcionários sem políticas de privacidade claras ou mecanismos de consentimento informado para indivíduos menores de 18 anos¹⁷⁶.

173. Fundación Acceso, “Observatorio Centroamericano de Seguridad Digital: Relatório Interanual 2020-2025 [Manuscrito em preparação]”.

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

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

176. InternetLab, “Tecnologias de Vigilância e Inteligência Artificial na Educação: Promessas de modernização, realidades de opacidade”, InternetLab (out. 2025). Disponível em: https://internetlab.org.br/wp-content/uploads/2025/10/relatorio_ia_28092025.pdf

Existem diversas iniciativas para implantar tecnologias de reconhecimento facial no **Brasil**. Entre elas, destaca-se a instalação de 17 pontos de busca com reconhecimento facial no Rio de Janeiro durante a celebração do Ano Novo de 2024 na praia de Copacabana¹⁷⁷ e a implantação de 12 câmeras adicionais de reconhecimento facial, drones e 18 pontos de controle nas vias de acesso, durante o show gratuito de Lady Gaga naquela mesma praia em maio de 2025, que contou com a presença de mais de 2,5 milhões de pessoas^{178 179}.

Na **Argentina**, o governo de Javier Milei criou a Unidade de Inteligência Artificial Aplicada à Segurança, que permite às forças federais patrulhar redes sociais e a dark web, analisar imagens de câmeras em tempo real usando reconhecimento facial, utilizar algoritmos para “prever” crimes futuros, criar perfis de suspeitos e patrulhar grandes áreas com drones¹⁸⁰. Em maio de 2025, o Plano Nacional de Inteligência revelou que a Secretaria de Inteligência do Estado pretendia monitorar os atores que gerassem “perda de confiança nas políticas econômicas” ou “manipulassem a opinião pública” nos processos eleitorais¹⁸¹.

No **Paraguai**, a organização de direitos digitais TEDIC documentou a expansão das câmeras de reconhecimento facial instaladas desde 2018 por pelo menos 13 instituições públicas, sem um marco legal que regule seu uso até o momento, sem estudos de impacto sobre os direitos humanos e com verbas do Fundo de Serviço Universal desviadas para financiar infraestrutura de vigilância¹⁸². No **Ecuador**, um decreto presidencial de setembro de 2024 estipulou que a ECU-911 assumiria o controle exclusivo das câmeras do governo local e implementaria um sistema de videovigilância em tempo real com reconhecimento facial e de placas de veículos¹⁸³.

Outra opção é a utilização de plataformas de análise de dados massivos. O **Ecuador** formalizou uma colaboração entre janeiro e maio de 2025^{184 185}. A empresa firmou parceria com a Palantir Technologies para implementar sua plataforma

177. Mariana Milanés, et al., “Reconocimiento facial y tecnologías de vigilancia en América Latina: casos, proveedores y dinámicas comerciales”, *Al Sur* (jun. 2025). Disponível em: <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] (2 maio 2025). Disponível em: https://www.instagram.com/derechos_digitales/p/DJKKV6ARFF4/

179. Douglas Corrêa, “Seguridad reforzada para concierto de Lady Gaga en Copacabana”, *Agência Brasil* (29 abr. 2025). Disponível em: <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* (jul. 2024). Disponível em: <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* (25 maio 2025). Disponível em: <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* (29 abr. 2025). Disponível em: 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* (18 set. 2024). Disponível em: <https://www.ecuavisa.com/ecuador/el-ecu-911-accedera-a-los-videos-de-las-cameras-de-seguridad-de-los-gad-tras-decreto-presidencial-20240918-0070.html>

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

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

de análise de dados no Serviço Nacional de Alfândega (SENAE), com o objetivo declarado de combater o contrabando e a fraude aduaneira. A Palantir é uma empresa americana cuja tecnologia, originalmente desenvolvida para operações de inteligência do governo dos EUA, permite o cruzamento massivo de dados de múltiplas fontes para identificar padrões e perfis de pessoas em tempo real. O contrato autoriza o SENA a consolidar dados de outras entidades públicas na plataforma Palantir¹⁸⁶. Isso amplia o processamento de informações para além do controle aduaneiro e, portanto, representa riscos significativos para a privacidade das pessoas e para o controle que elas têm sobre seus próprios dados.

Por fim, outra dimensão da vigilância digital documentada na região é o monitoramento do discurso nas redes sociais. **Derechos Digitales** documentou duas práticas implementadas por governos na região¹⁸⁷: perfilamento, que consiste em caracterizar os usuários de mídias sociais de acordo com o fato de suas postagens serem favoráveis, críticas ou contrárias ao governo; e patrulhamento cibernético, que envolve o monitoramento secreto da atividade on-line para identificar e processar criminalmente pessoas por suas atividades na internet. Ambas operam sob a premissa de que qualquer conteúdo publicado na internet pode ser usado livremente pelo Estado, inclusive para fins de perseguição, o que tem sido questionado por organizações de direitos humanos¹⁸⁸.

Na **Colômbia**, uma investigação revelou que o governo contratou uma empresa para melhorar sua imagem perante o público; na prática, isso resultou na criação de uma lista com 486 usuários do X, classificados de acordo com sua posição favorável, neutra ou de oposição ao governo. No **Brasil**, em 2024, foi lançado um concurso público federal para a contratação de serviços de criação de perfis em redes sociais, justificado como uma ferramenta para medir a popularidade do governo, analisar as emoções dos usuários por meio de inteligência artificial e combater a desinformação¹⁸⁹.

No **México**, uma investigação de 2024 baseada em documentos vazados pelo coletivo Guacamaya revelou que o Ministério da Defesa adquiriu o software israelense HIWIRE em 2020 para monitorar usuários críticos das forças armadas em tempo real, mapear suas interações e criar contas falsas para interagir secretamente com alvos¹⁹⁰.

A prática de patrulhamento cibernético se espalhou por toda a região com diferentes níveis de regulamentação e opacidade: no **Uruguai**, a Direção-Geral da Polícia reconheceu em 2024 que monitorava redes sociais. Naquele mesmo ano, um

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* (ago. 2024). Disponível em: 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* (9 maio 2025). Disponível em: <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* (ago. 2024). Disponível em: https://www.derechosdigitales.org/wp-content/uploads/Informe-RELE-vigilancia-masiva_cerrado.pdf

190. Ibid.

adolescente foi preso após ser identificado erroneamente como participante de confrontos em centros educacionais, por ter sido confundido com um homônimo nas redes sociais¹⁹¹.

Em outros países, o patrulhamento cibernético foi incorporado ou reintegrado aos marcos regulatórios: na **Argentina**, foi reintegrado às normas locais em 2024, após ter sido revogado em 2022; no **Paraguai**, foi incorporado à lei de reforma e modernização da Polícia Nacional em junho de 2024¹⁹².

191. Ibid.

192. Ibid.

5. Conclusões



5 Conclusões

O projeto *Na mira 2* busca preencher uma lacuna na documentação regional sobre incidentes de segurança digital e práticas de vigilância, analisada de maneira sistematizada e sob a perspectiva dos direitos humanos e do interesse público. A informação existe e é valiosa; no entanto, se encontra dispersa por diversas fontes, sem um espaço que as integre e lhe dê significado a nível regional. Portanto, o valor deste exercício reside não em oferecer um ranking de países, mas em reunir, ordenar e dar significado a casos que, vistos isoladamente, podem parecer desconexos, mas que, em conjunto, nos permitem identificar atores, tecnologias, tendências regionais de impacto e traçar trajetórias ao longo do tempo.

Nesse sentido, os casos documentados não devem ser interpretados como uma amostra representativa ou como uma comparação direta entre países. A maior ou menor ocorrência de incidentes em um país pode ser atribuída a múltiplos fatores, como a capacidade de monitoramento das organizações locais, as circunstâncias específicas do período ou mudanças de governo que alteram drasticamente o cenário de um ano para o outro. Comparar números entre países sem considerar essas variáveis pode levar a conclusões incorretas.

A vigilância, a perseguição a jornalistas e ativistas e o fechamento do espaço cívico dificultam diretamente o trabalho de organizações que monitoram esses fenômenos, como é o caso da Nicarágua, onde mais de 2.600 organizações da sociedade civil foram dissolvidas entre 2018 e 2022¹⁹³. Mas mesmo em países com instituições mais consolidadas, como a Argentina e o México, observa-se uma tendência crescente de restringir o acesso à informação, o que representa uma preocupação regional que transcende as classificações usuais entre democracias e regimes autoritários.

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

Mesmo com essas limitações, o relatório demonstra que os incidentes de segurança digital não podem ser analisados como eventos puramente técnicos; os casos documentados respondem a contextos políticos específicos. Portanto, as iniciativas de segurança digital que não levam em consideração esse contexto correm o risco de oferecer respostas parciais: proteger um dispositivo não protege totalmente uma pessoa cuja organização está sendo perseguida pelo Estado, nem um jornalista cujo veículo de comunicação foi fechado. Compreender essa dimensão é essencial para que as respostas de segurança digital sejam verdadeiramente eficazes.

O relatório também destaca uma tensão preocupante entre a rápida adoção ou legitimação de tecnologias e práticas de controle e o ritmo lento com que os mecanismos de transparência e proteção de direitos estão avançando. Em particular, há tentativas de validar legalmente práticas como o patrulhamento cibernético ou de expandir as capacidades de análise e vigilância do Estado, sem que isso seja acompanhado, na mesma medida, por mecanismos proporcionais de controle e responsabilização.

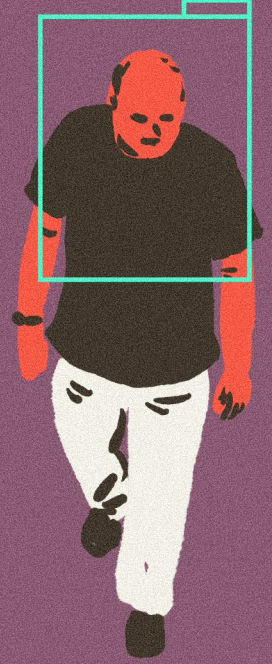
Um elemento que distingue este relatório da sua edição anterior é a crescente presença da IA como um vetor transversal nos incidentes documentados. Sua presença em múltiplas seções reflete o desafio de compreender a IA não apenas como uma ferramenta para a inovação, mas como parte de infraestruturas mais amplas de poder, classificação, controle e produção de danos, cujos efeitos não recaem uniformemente sobre todas as pessoas. Um exemplo claro é a geração de deepfakes sexualizados, que se tornou uma prática de violência e controle dirigida particularmente contra as mulheres. No entanto, é importante ressaltar que o surgimento dessas novas tecnologias não substitui as formas mais tradicionais de repressão e controle. Na América Central, por exemplo, persiste um conjunto de múltiplos mecanismos que combinam ferramentas tecnológicas, reformas legais restritivas e perseguição política, operando simultaneamente e reforçando-se mutuamente.

Ao longo deste relatório, fica claro que os impactos dos incidentes não estão distribuídos de maneira homogênea. Jornalistas, ativistas, opositores políticos, mulheres, pessoas LGBTQIA+, comunidades migrantes, populações empobrecidas ou pessoas com menos acesso a recursos digitais enfrentam riscos específicos dependendo do tipo de tecnologia ou ataque. Em diversos casos, o impacto transcende o indivíduo e produz efeitos coletivos, como a autocensura, a inibição de protestos, o enfraquecimento das redes de apoio ou a redução do espaço cívico.

Essa distribuição desigual de impactos pode ser atribuída tanto a atores estatais quanto privados. Por exemplo, os primeiros utilizam software de vigilância para perseguir opositores políticos. Entretanto, no setor privado, há casos notáveis como o da World, que compra dados biométricos em larga escala, ou aplicativos de empréstimo que implementam mecanismos de extorsão; dois casos que ilustram como a tecnologia é usada para tirar proveito das condições econômicas da população.

Por fim, cabe destacar que o fim do financiamento por parte do governo dos Estados Unidos e o encerramento da USAID em 2025¹⁹⁴ tiveram um forte impacto nas organizações da sociedade civil da região. Essa situação dificultou a coordenação dos trabalhos do OLAD e atrasou a publicação deste relatório. No entanto, o apoio constante de seus membros foi fundamental para a conclusão deste relatório, e gostaríamos de agradecer a colaboração deles no desenvolvimento do *Na mira 2*.

194. Débora Calderón, “Recalculando: nuevas estrategias para enfrentar los ajustes en la cooperación internacional”, *Derechos Digitales* (11 jul. 2025). Disponível em: <https://www.derechosdigitales.org/recursos/recalculando-nuevas-estrategias-para-enfrentar-los-ajustes-en-la-cooperacion-internacional/>



 Derechos
Digitales
AMÉRICA LATINA

