Na mira: segurança e principais ameaças digitais na América Latina

DERECHOS DIGITALES
América Latina

NA MIRA: SEGURANÇA E PRINCIPAIS AMEAÇAS DIGITAIS NA AMÉRICA LATINA

Esta publicação foi realizada por Derechos Digitales, uma organização independente e sem fins lucrativos, fundada em 2005, que tem como missão a defesa, promoção e desenvolvimento dos direitos fundamentais em ambientes digitais na América Latina.

Supervisão geral: Rafael Bonifaz e Mayra Osorio

Autor: Valentín Díaz

Revisão e correção de textos: Rafael Bonifaz, Mayra Osorio e Juan Carlos Lara

Tradução para inglês e português: Inglés-Gonzalo Bernabó / Português-Dafne Melo

Design:Alter Studio

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

dezembro de 2024

Sumário

NA MIRA: SEGURANÇA E PRINCIPAIS AMEAÇAS DIGITAIS NA AMÉRICA LATINA

RELATÓRIO — DEZEMBRO DE 2023 A MAIO DE 2024

1.INTRODUÇÃO

A defesa dos direitos humanos no espectro digital é uma tarefa que tem sido repleta de obstáculos na América Latina, em meio a um aumento de governos que utilizam a tecnologia como uma arma contra a dissidência política e de uma presença crescente de criminosos online. Nesse panorama, ocorrem ataques cibernéticos com efeitos nos serviços públicos, coleta massiva e abuso de dados pessoais por entidades públicas e privadas, espionagem estatal e assédio dirigido a diversas comunidades em risco como defensores dos direitos humanos e das diversidades, ativistas e jornalistas. Essas são apenas algumas das ameaças online e das violações dos direitos humanos a que os atores da sociedade civil estão expostos na região mais perigosa do mundo para líderes sociais (Tarazona, 2024).

A internet tornou-se um espaço essencial para o exercício do ativismo e a defesa dos direitos humanos, motivo pelo qual mantê-la livre, aberta e segura torna-se imperativo para garantir o exercício dos direitos. Portanto, num contexto hostil à escala regional, a defesa dos direitos humanos no espaço digital exige esforços transfronteiriços cada vez maiores. Particularmente no campo da segurança e análise de ameaças digitais com uma abordagem social crítica, o monitoramento e a atenção aos casos por parte de diferentes organizações carecem de compilação e sistematização como fenômenos regionais.

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 trabalham na defesa dos direitos humanos online,

que decidiram unir forças para melhorar a compreensão do comportamento dos incidentes de segurança digital a partir de uma perspectiva regional.

O OLAD começou a ser formado em 2021 e passou por diversos processos de amadurecimento até a publicação deste relatório. Hoje fazem parte dessa aliança as organizações Código Sur (regional), Colnodo (Colômbia), Conexión Segura (Venezuela), Derechos Digitales (regional), Escola de Ativismo (Brasil), Fundación Acceso (regional), Fundación InternetBolivia.org (Bolivia), Fundación Karisma (Colômbia), Instituto Nupef (Brasil), LaLibre.net Tecnologías Comunitarias (Equador), MariaLab (Brasil), Social TIC (México), Sursiendo (México) e Taller de Comunicación Mujer (Equador).

Cada uma das organizações do OLAD desempenham funções diferentes nos seus respectivos espaços geográficos e nos contextos particulares de cada país. Enquanto alguns deles se concentram, por exemplo, na investigação e acompanhamento de casos de ciberespionagem ou censura de ativistas e jornalistas, outros dedicam seus esforços à democratização da tecnologia e à proteção de grupos em situações de vulnerabilidade ou marginalização histórica diante dos ataques em espaços digitais que, por sua vez, são expressões de preconceitos baseados em múltiplas desigualdades de gênero, raça, classe social, identidade sexual, idade ou condição de deficiência.

Em outubro de 2023, vários membros do OLAD tiveram uma reunião presencial em Santiago, Chile, onde concordaram em realizar o relatório Na mira, um monitoramento colaborativo de incidentes de segurança digital. Este relatório compila, assim, o trabalho articulado dessas organizações, num período definido entre dezembro de 2023 e maio de 2024. Da mesma forma, pretende contribuir com a observação dos processos do Observatório, identificando pontos fortes e desafios para o futuro, tendo em conta as complexidades típicas do trabalho colaborativo.

2. METODOLOGIA

O relatório *Na mira* é construído sob uma metodologia mista, que mescla a análise de dados coletados no cotidiano das organizações com experiências qualitativas decorrentes de discussões nas diferentes fases de trabalho com o Observatório.

Para isso, foram desenhadas duas formas de coletar as informações. O primeiro é um esforço conjunto para monitorar o contexto em questões de segurança digital na América Latina, que para fins de compreensão deste relatório será doravante denominado "monitoramento de contexto". A segunda é uma esquematização de uma série de dados compilados a partir dos casos abordados por cada organização que faz parte do OLAD, que este relatório chamará de "relatório de casos próprios". Para ambos os processos foi delimitado um período de coleta de informações de dezembro de 2023 a maio de 2024.

Para monitorar o contexto, a equipe do OLAD recolheu uma série de entradas de informação documental. Foi realizada uma curadoria de artigos de imprensa e publicações da sociedade civil sobre incidentes e ameaças digitais relevantes registrados na América Latina durante o período indicado e foram elaborados relatórios mensais que facilitaram uma análise geral do que aconteceu nesses seis meses. Entre os incidentes analisados estão os ciberataques que afetaram infraestruturas públicas e serviços estatais nos países estudados, situações de cyberbullying e censura de ativistas, bem como graves violações dos direitos humanos por meio da utilização de tecnologias de vigilância contra a sociedade civil, entre outros fatos relevantes.

Por outro lado, o relato de casos próprios consiste na coleta de dados com base nos casos abordados por cada uma das organizações participantes no OLAD, a partir de mecanismos próprios, protocolos de atendimento e medidas de anonimização de dados. Sendo o Observatório uma união de organizações de diferentes naturezas que trabalham em diferentes contextos, os dados recolhidos para o relato dos seus casos próprios são igualmente diversos, pelo que não devem ser vistos como uma medida comparativa entre casos, países ou organizações.

É necessário destacar que o relatório apresenta um viés de limitação relacionado às linhas temáticas de cada organização que faz parte do OLAD, razão pela qual as cifras e números apresentados no relatório de casos próprios devem ser analisados sob perspectivas diferentes da tendência natural desse tipo de relatórios para gerar ranqueamentos. Pelo contrário, estes dados devem ser analisados como uma representação do trabalho de atenção de casos que realizados pelas organizações pertencentes ao Observatório.

Apesar dessas dispersões, a equipe do OLAD conseguiu identificar quatro problemáticas comuns que as organizações que fazem parte do projeto abordam. Trata-se de vigilância e espionagem, violência de gênero em espaços digitais, ataques a

infraestruturas críticas e violações da liberdade de expressão online nos países onde as organizações trabalham.

Os casos documentados pelas organizações entre 2023 e 2024 foram divididos em três períodos. O primeiro relatório coletou dados entre dezembro de 2023 e janeiro de 2024 e coletou 163 casos; o segundo foi realizado de fevereiro a março de 2024, com 135 casos; e um último de abril a maio de 2024, que contabilizou 113 casos. No total, foram 411 casos atendidos pelas organizações, no período de dezembro de 2023 a maio de 2024.

3. CONTEXTO DE SEGURANÇA DIGITAL NA AMÉRICA LATINA

Esta seção oferece uma visão do panorama conjuntural de violações e incidentes de segurança digital que ocorreram na região durante o período coberto. Este capítulo, conforme indicado na seção metodológica, foi construído com base em uma seleção de artigos de imprensa e relatórios sobre casos de ataques e violações digitais de grande magnitude ou impacto social e que, por sua vez, afetaram diferentes grupos historicamente discriminados. Vale ressaltar que os incidentes detalhados nessa seção não correspondem a todos os eventos registrados na região durante o período designado, mas são uma amostra que resulta de um trabalho constante de monitoramento.

3.1 BOLIVIA

Durante o período coberto por este relatório, a Bolívia viveu um dos períodos mais intensos de polarização política dos últimos anos. Uma ruptura evidente no partido no poder (Molina, 2023) separou os leais ao governo de Luis Arce daqueles que permaneceram na linha do ex-presidente Evo Morales. Entretanto, em junho de 2024, uma tentativa fracassada de golpe de Estado (BBC News Mundo, 2024) tensionou ainda mais a já dividida opinião pública.

Com 62% da sua população autorreconhecida como indígena (Instituto Nacional de Estatística da Bolívia, 2024), o músculo social da política partidária boliviana baseia-se em sua população rural. A situação política nacional também tem impacto na organização comunitária, uma vez que o atual partido no poder tem origem em organizações de base com enfoque plurinacional (Do Alto, 2007).

Em maio de 2024, a LatAm Journalism Review publicou uma compilação de pesquisas de organizações locais que estudaram o fenômeno da desinformação que se espalha em comunidades rurais na Bolívia, Peru e El Salvador (Knoerr, 2024). Particularmente na Bolívia, segundo uma investigação do ChequeaBolivia, em três localidades rurais (Villa Tunari, Cochabamba; Yacapaní e Montero, Santa Cruz) a desinformação online intensificou-se durante a crise política e eleitoral de 2019, que culminou com a saída de Evo Morales do poder e protestos massivos, com grande participação de organizações rurais, contra o governo de transição de Jeanine Añez que deixou dezenas de mortos (ChequeaBolivia, 2024). O relatório mostra que a população indígena, durante esses acontecimentos, esteve particularmente exposta à desinformação. Já num novo governo, mas ainda num contexto polarizado, as comunidades rurais poderão ser sujeitas a novas tentativas de manipulação do discurso público.

3.2 BRASIL

Em abril de 2024, a justiça brasileira abriu uma investigação contra o magnata Elon Musk, acionista majoritário do X (ex-Twitter), e o apontou como o responsável de uma "instrumentalização criminal" para obstruir a justiça (*Folha de S. Paulo*, 2024) após a reativação de diversas contas de usuários que o judiciário havia ordenado encerrar, por considerá-las amplificadoras de desinformação. Musk então respondeu com uma série de desqualificações públicas do juiz que tomou a decisão (DW, 2024). O evento aprofundou a crise nas relações entre a plataforma e o governo, que culminou com a suspensão temporária da rede social em escala nacional por ordem de um juiz do Supremo Tribunal Federal (STF), sob a exigência de que a empresa nomeasse um representante legal no Brasil, o segundo maior mercado de X no mundo (BBC News Mundo, 2024).

Soma-se a esse panorama o fato de Elon Musk também ser dono da empresa de internet via satélite Starlink, cujo volume de tráfego segundo o relatório anual Cloudflare Radar 2023 triplicou naquele ano no Brasil, especialmente em áreas rurais sem cobertura (Belson, 2023). O governo procurava alternativas a essa dependência e em novembro de 2024 assinou um memorando com a China para utilizar a sua constelação de satélites comerciais para oferecer ligação de banda larga a áreas remotas (Xinhua Español, 2024).

Os conflitos jurídicos entre o governo brasileiro e o X ocorreram depois da mudança de proprietário da plataforma após um complexo processo de compra hostil por parte de Musk (BBC News Mundo, 2024) Em 2022, a plataforma então chamada Twitter concordou com uma série de regulamentações restritivas ordenadas pelo Tribunal Superior Eleitoral (TSE) do Brasil para proteger as eleições presidenciais do impacto da desinformação. A regulamentação deixou nas mãos do tribunal a decisão sobre quais conteúdos deveriam ser retirados da plataforma, sob pena de multas elevadas por cada hora de atraso nos esforços de moderação (Chambers, 2022).

O então presidente Jair Bolsonaro e vários de seus apoiadores vinham se manifestando constantemente, há algum tempo, sobre suposta falta de transparência do TSE e, em diversas ocasiões, levantaram dúvidas sobre a confiabilidade do sistema de votação eletrônica do país (Díaz, 2022). Apesar das restrições impostas pelo TSE aos principais palanques e do silêncio que Bolsonaro manteve após a divulgação dos resultados que declararam Lula vencedor, no dia 8 de janeiro de 2023, milhares de seguidores do candidato derrotado eleitoralmente invadiram e vandalizaram os prédios do Congresso, a Presidência da República e o Supremo Tribunal Federal (STF) (BBC News Mundo, 2024). Após a compra de Musk, o Supremo Tribunal de Justiça abriu investigação contra o magnata por supostamente não conter desinformação direcionada ao TSE (Biller & Sá Pessoa, 2024).

Também em abril, uma extensa investigação do The Influence Industry Project analisou como a desinformação eleitoral nas plataformas Meta (Facebook, Whatsapp e Instagram) desempenhou o seu papel nas tentativas de desestabilização democrática de 2023 (Maia, 2023). Em maio, o judiciário brasileiro assinou um acordo de entendimento com diversas empresas, incluindo Meta, TikTok, Google, Kwai e LinkedIn, para redobrar esforços contra a desinformação (Abrão, 2024).

A corresponsabilidade das plataformas quanto à integridade eleitoral, à defesa da democracia e à confiança nas instituições democráticas do país são questões amplamente discutidas no Brasil. Nessa busca, há vários anos os diferentes poderes do Estado tem adotado regulamentações e instalado debates parlamentares e também direcionados à sociedade civil (Global Freedom Of Expression Columbia University, 2020). Ao longo desse caminho, o Brasil encontrou não apenas a resistência frontal de Musk, mas também o lobby constante gerado por um punhado de grandes empresas de tecnologia (big techs) para desacelerar ou implodir projetos regulatórios (Colombo, 2024). Em janeiro de 2024, por exemplo, a Polícia Federal concluiu após investigação um "abuso de poder econômico" por parte do Google e do Telegram contra a aprovação de um projeto de lei contra a desinformação (Falcão, 2024). Num delicado equilíbrio entre

a saúde da democracia brasileira e a liberdade de expressão, a desinformação continua sendo um dos principais desafios de um Brasil interligado.

Em dezembro de 2023, o governo fez um avanço importante em termos de privacidade, lançando um aplicativo que permite às vítimas de roubo bloquear remotamente os seus dispositivos, função que facilita os procedimentos de denúncia e permite às vítimas proteger rapidamente informações sensíveis (EFE, 2023).

Em matéria legislativa, desde o final de 2023, o Senado vem discutindo um projeto de marco regulatório sobre inteligência artificial (Projeto de Lei n. 2338, 2023), regulamentação que, até o momento, organizações locais de direitos humanos e tecnologia têm visto com bons olhos (Coalizão Direitos Na Rede, 2024). Em 2024, o Conselho de Comunicação Social do Congresso Nacional reuniu-se para discutir projetos de lei que visam tornar os conteúdos jornalísticos sujeitos a remuneração pelas plataformas onde são partilhados (Câmara dos Deputados, 2024).

Em janeiro de 2024, a Polícia Federal anunciou uma investigação contra ex-funcionários da Agência Brasileira de Inteligência (Abin) durante o governo Bolsonaro, a quem acusa de ter vigiado ilegalmente cerca de 30 mil pessoas, entre jornalistas e magistrados do STF (Sadi, 2024). As denúncias envolvem o deputado federal Alexandre Ramagem, que foi diretor da entidade no governo Bolsonaro, supostamente responsável pelo uso ilegal de um software de origem israelense chamado FirstMile da empresa Cognyte, que permite interceptar a posição geográfica de um dispositivo móvel através de seus sinais GPS, por meio de alteração do protocolo SS7 gerenciado pelas empresas de telecomunicações do país, informação confidencial por lei (BBC News Brasil, 2024).

Em março de 2024, uma investigação do *Intercept Brasil* revelou o uso de uma ferramenta que permite a coleta de informações de inteligência de código aberto (OSINT) em perfis privados no Facebook, por mais de uma dezena de organizações públicas (Ameno, 2024). Uma constatação que trouxe novamente à tona o papel dos governos e os limites da coleta de dados pessoais em prol da segurança dos cidadãos.

3.3 COLÔMBIA

A Colômbia começou o ano de 2024 perdendo a oportunidade de aprovar um projeto legislativo sobre tecnologia com perspectiva de gênero. O projeto foi colocado em debate em janeiro e teve origem em uma ordem da Corte Constitucional para que o Estado passasse a abordar a violência de gênero no espaço digital (Moreno, 2022). Mas durante os debates no

parlamento (Castañeda, 2022), a proposta inicial foi sujeita a alterações que ressignificaram completamente o conceito inicial da lei, a proteção das pessoas expostas à violência de género (Karisma, 2024). Em maio, mudando apenas a ordem de três palavras, o Legislativo deixou a porta aberta para uma nova gama de definições de violência digital (Moreno, 2024), que inclui menções à proteção de funcionários públicos que levantam suspeitas da comunidade defensora dos direitos humanos em ambientes digitais[1].

Por outro lado, em fevereiro, o governo de Gustavo Petro procurou um rumo para a transformação digital ao apresentar a sua Estratégia Nacional Digital para 2026 (Ministério das TIC, 2024). A estratégia concebe a transformação digital como uma política holística que foi dividida em quatro pilares: conectividade; infraestrutura de dados; confiança e segurança digital; habilidades ou fomento de talento digital.

No início do ano de 2024, um ataque cibernético do tipo ransomware[2] aos portais da seguradora médica Salud Total gerou interrupções no atendimento em um sistema com 4,8 milhões de membros (Rodríguez, 2024). A Superintendência Nacional de Saúde teve que se manifestar, num país onde o sistema público de saúde é gerido por prestadores privados.

Em março de 2024, o jornalista israelense Gur Meggido, do jornal Haaretz, afirmou em uma investigação que a Colômbia pagou 13 milhões de dólares em dinheiro pela aquisição do software espião Pegasus, do grupo israelense NSO (Megiddo, 2024). Meses depois, essa mesma informação foi denunciada pelo presidente Gustavo Petro (Beltrán, 2024), que culpou seu antecessor Iván Duque pela compra em 2021, quando a Colômbia vivia protestos massivos que duraram vários meses.

Em abril, o ministro da Defesa Iván Velásquez reconheceu (Revista Semana, 2024), após a publicação de uma investigação jornalística (AFP, 2024), a presença no TikTok de perfis associados ao maior grupo de frentes dissidentes da extinta guerrilha das FARC, o Estado-Maior Central (EMC). Na rede social de origem chinesa, os guerrilheiros enviam mensagens de recrutamento dirigidas à juventude colombiana. O general Hélder Giraldo, então comandante-geral das Forças Militares, garantiu que a atuação dos dissidentes naquela rede

1 Tanto a primeira versão do projeto, proposta na Comissão Primeira Constitucional Permanente do Senado, como as versões subsequentes com as modificações mencionadas neste relatório aparecem no diário oficial do Congresso da Colômbia. Em sua primeira versão, aparece no diário N 605 de 2023. A versão mais recente, que acabou sendo arquivada, consta no diário N 342 de 2024. Ambos podem ser localizados no mecanismo de busca do Diário do Congresso (Congresso da República da Colômbia, s/f).

2 Ransomware: Malware que bloqueia um dispositivo mediante o cifrado ou criptografando seu conteúdo. Tem fins de extorsão, pois é solicitado resgate para divulgação das informações (ESET, s/f).

social representa “uma flagrante violação do mesmo cessar-fogo” que naquela altura regia a realização de ciclos de conversações de paz com o governo colombiano.

3.4 EQUADOR

Recentemente, a crise de segurança no Equador atingiu novos níveis e deixou uma taxa recorde de homicídios de 47 por 100 mil habitantes em 2023 (Observatorio Ecuatoriano de Crimen Organizado, 2024), a mais alta da América Latina. Entre os acontecimentos violentos mais relevantes estão o assassinato do candidato presidencial Fernando Villavicencio em agosto de 2023 (BBC Mundo, 2023) e a onda nacional de violência armada que o país viveu em janeiro de 2024 (Cañizares et al., 2024), que se espalhou globalmente devido à tomada de reféns de trabalhadores da estação de televisão estatal TC por um grupo armado durante uma transmissão.

Esses últimos acontecimentos levaram o presidente Daniel Noboa a decretar o estado de conflito armado interno, o que permitiu a militarização do país (BBC News Mundo, 2024). Essa situação deu origem a uma série de violações dos direitos humanos, cometidas principalmente por militares, incluindo casos de execuções extrajudiciais, desaparecimentos forçados e centenas de denúncias de tortura nas ruas e prisões do país (Human Rights Watch, 2024). Ao mesmo tempo, o governo empreendeu uma campanha difamatória contra os defensores dos direitos humanos que foram expostos à narrativa oficial (Anistia Internacional, 2024), uma apologia aos abusos militares que também foi amplamente difundida pelos utilizadores nas redes sociais durante os primeiros meses do declaração de conflito (Curipoma, 2024).

Nesse contexto, o Comitê Permanente de Defesa dos Direitos Humanos (CDH Guayaquil), que representa, entre dezenas de vítimas de violações de direitos humanos em Guayaquil, famílias de pessoas privadas de liberdade, denunciou em fevereiro um ataque cibernético que desabilitou seus e-mails, que a organização descreveu como “um ato deliberado de intimidação, resultado de denúncias de abusos por parte das Forças Armadas” (@cdh.gye, 2024). No mesmo mês, a ONG de proteção a jornalistas Fundamedios enviou um alerta sobre uma série de ataques cibernéticos, mais de 300 desde dezembro de 2023, contra o portal jornalístico Indómita Media, que publica permanentemente sobre a deterioração da situação dos direitos humanos no Equador (Fundamedios, 2024).

Como antessala desses acontecimentos, em dezembro de 2023, um caso judicial ligado a um narcotraficante falecido abalou as investigações sobre o assassinato do candidato

presidencial Fernando Villavicencio (Fiscalía General del Estado Equador, 2024). Em conversas extraídas do telefone de Leandro Norero, chefão do crime assassinado em um massacre penitenciário em 2022 (BBC News Mundo, 2024), ficaram evidentes ligações entre o traficante de drogas e trabalhadores do ECU-911, centro estatal de atendimento e coordenação de emergências que gerencia uma extensa rede nacional de câmeras de vigilância (ECU-911, s/fa).

Para o chamado caso Metástase, a Procuradoria-Geral do Estado divulgou uma série de registros de conversas do aplicativo Threema, de Norero, com diversas figuras públicas, incluindo jornalistas, policiais, guias penitenciários e funcionários judiciais. Um dos chats divulgados mostrou que Norero utilizou software do sistema nacional de atendimento de emergência, ECU-911, para monitorar Villavicencio (Bonifaz, 2024), informação que posteriormente foi reconhecida pelo diretor da entidade como um caso de "uso indevido" de suas tecnologias em janeiro de 2024 (Primicias, 2024). O programa utilizado foi o Mobile Locator, um software de geolocalização que, segundo a própria ECU-911, oferece um "posicionamento aproximado da chamada feita por uma pessoa para a linha única de emergência 911 de um telefone" (ECU-911, s/fb).

Paralelamente, a Assembleia Nacional do país tentou tramitar uma lei de segurança digital que estabelecesse pela primeira vez um debate que abordasse a prevenção e tratamento de ameaças digitais e ataques cibernéticos. Sem estar isento de artigos polêmicos (Carrillo, 2024), o projeto pioneiro significou pelo menos uma aceleração do debate público sobre segurança cibernética. Porém, o projeto acabou arquivado por falta de apoio político (Asamblea Nacional del Ecuador, 2024).

Em dezembro de 2023, a Controladoria-Geral do Estado iniciou uma auditoria do processo de contratação para a instalação de um sistema de votação online destinado à comunidade migrante de equatorianos no exterior para o primeiro turno das eleições de agosto daquele ano (El Universo, 2023). A implementação dessa tecnologia foi um fracasso (La Barra Espaciadora, 2024), pois a plataforma entrou em colapso e os usuários registraram problemas desde a madrugada no exercício do direito de voto. Posteriormente, a presidente da organização, Diana Atamaint, garantiu que a plataforma tinha sido alvo de um ataque cibernético, pelo que foi decidido suspender a contagem dos votos e ignorar os resultados para aquela população. Posteriormente, soube-se que a empresa contratada não possuía experiência no ramo.

Por outro lado, na esfera judicial, chegou ao fim em 2024 o emblemático caso do cientista da computação sueco Ola Bini, acusado pelo Ministério Público equatoriano por alegações amplamente questionadas por organizações da sociedade civil (Bonifaz

& Silva, 2024), embora não com o resultado que as suas organizações de defesa e de direitos humanos esperavam. Numa estranha reviravolta e com um argumento sem precisão técnica, um tribunal de apelação reverteu uma sentença de primeira instância que o declarava inocente do crime de acesso não consensual a um sistema informático (CNN Español, 2024b). Com essa condenação, o cientista enfrentaria um ano de prisão, mas dias depois o mesmo tribunal aceitou um pedido de suspensão condicional da pena. Ou seja, Ola Bini é um homem livre, embora condenado pela justiça. O sueco foi detido em circunstâncias questionáveis (Electronic Frontier Foundation, 2021), pois a sua prisão coincidiu com a expulsão do fundador do Wikileaks, Julian Assange, da embaixada do Equador no Reino Unido, onde o australiano tinha obtido asilo desde 2012. Ola Bini e Julian Assange eram amigos íntimos e o então presidente Lenín Moreno, juntamente com a sua Ministra do Interior, María Paula Romo, ligaram o sueco a alegadas tentativas de desestabilização.

3.5 EL SALVADOR

El Salvador, por sua vez, vive um suposto processo de erosão de sua democracia sob o governo de Nayib Bukele (Bernal, 2024), que foi reeleito em 2024 com a aprovação do Tribunal Supremo Eleitoral, apesar de uma expressa proibição constitucional (CNN Espanhol, 2024). Tal como nos casos da Venezuela e da Nicarágua, mencionados mais adiante, esses processos sociais têm repercussões no espectro digital.

Já em 2022, a Human Rights Watch alertou (Taraciuk, 2022) sobre a aprovação de uma bateria de reformas legais pela Assembleia Legislativa que incluiu modificações ao Código Penal e à Lei de Delitos Informáticos (Derechos Digitales, 2022), que tornam a categoria de crimes cibernéticos, condutas como a obtenção de material confidencial, entre outras, o que coloca em risco a prática jornalística.

Em 2023, o país ficou em 115º lugar entre 180 no índice de liberdade de imprensa da Repórteres Sem Fronteiras (RSF) e em 2024 caiu 18 posições e ficou em 133º lugar (RSF, 2024). Como pano de fundo, em 2022, o Citizen Lab da Universidade de Toronto publicou uma extensa investigação na qual revelou violações ilegais do spyware Pegasus nos telefones de representantes de organizações da sociedade civil e jornalistas, entre essas pessoas, 22 jornalistas do portal investigativo *El Faro* (Gavarrete et al., 2022).

No final daquele ano, um grupo de trabalhadores da mídia entrou com uma ação judicial contra a empresa em um tribunal dos EUA. Mas em março de 2024, o processo foi indeferido por um juiz da Califórnia. No seu apelo, o grupo de jornalistas obteve o apoio dos gigantes Microsoft e Google, dois fabricantes cujos produtos foram violados pela Pegasus para o acesso às comunicações dos funcionários do *El Faro* (Gressier, 2024)

3.6 MÉXICO

Nos últimos dois anos, o México tentou aprovar legislação relacionada com os direitos humanos no âmbito digital, segurança cibernética e assédio digital, sem muito sucesso na promoção e discussão destas ideias, tanto que três projetos federais propostos pelos legisladores estão paralisados, sem avanços (Reis, 2024).

Em janeiro de 2023, um banco de dados pessoal sensível de vários repórteres circulou em um fórum de vazamentos (Osorio, 2024). Mais tarde soube-se que a base de dados provinha do sistema de acreditação de imprensa da Presidência para entrar nas conferências matinais do ex-Presidente Andrés Manuel López Obrador. Isso ocorreu num contexto delicado para a prática do jornalismo, uma vez que o México é o país mais perigoso sem guerra para a prática do jornalismo (RSF, 2024).

Em fevereiro, o país ganhou as manchetes com uma nova situação de vigilância excessiva quando uma investigação do R3D revelou algumas das atividades do Centro de Operações do Ciberespaço (COC) (R3D, 2024a), anexo ao Ministério da Defesa Nacional, que sob a fachada de "operações militares no ciberespaço" monitoraram a atividade de usuários críticos do exército nas redes sociais, numa tentativa de influenciar a opinião pública, inclusive por meio de contas de robôs.

Nesse mesmo mês, o Estado enfrentou novo escrutínio devido ao caso Pegasus (Artigo 19, 2024), quando o Supremo Tribunal de Justiça ordenou ao Ministério das Finanças que tornassem públicas as informações recolhidas para uma investigação realizada por essa entidade sobre a compra e utilização do spyware israelense objeto de centenas de denúncias de governos que utilizaram a ferramenta para perseguir ativistas, jornalistas e dissidentes políticos. Com um progresso muito lento, o caso Pegasus no México está longe de estar encerrado.

Um mês antes, o único processado pela intervenção ilegal com Pegasus no telefone da jornalista Carmen Aristegui, o operador Juan Carlos García, havia sido absolvido por um juiz federal que considerou que a Procuradoria-Geral da República não conseguiu

provar sua participação no delito (Proceso, 2024). O juiz, no entanto, reconheceu que a jornalista foi interceptada ilegalmente e considerou que o caso deveria continuar a ser investigado porque o Ministério Público não tem feito esforços suficientes para fazer justiça.

Por outro lado, em abril de 2024, a gigante de crédito e comércio varejista, Coppel, foi amplamente questionada por organizações da sociedade civil por se manter silenciosa diante de um ataque cibernético que afetou massivamente os seus serviços e cujas características técnicas nunca foram esclarecidas aos consumidores (R3D, 2024). Vozes independentes garantiram que deve ter sido um ataque do tipo ransomware.

3.7 NICARÁGUA

O saldo da medição dos direitos humanos em ambientes digitais na Nicarágua é negativo, como já observado num relatório emitido em setembro de 2023 (Derechos Digitales, 2023). O documento aponta antecedentes importantes que remontam aos protestos massivos e prolongados de 2018 que foram brutalmente reprimidos pelo governo de Daniel Ortega (OEA, 2018).

Um relatório desse ano da Comissão Interamericana de Direitos Humanos (CIDH) menciona graves violações dos direitos humanos que incluem execuções extrajudiciais, casos de tortura e centenas de detenções arbitrárias, bem como atos de censura contra cidadãos, jornalistas e meios de comunicação (Comissão Interamericana de Direitos Humanos, 2018).

Paralelamente, a repressão também esteve presente no espaço digital e ações como a interrupção do acesso à Internet, a criminalização da expressão online, as tentativas de manipulação da opinião pública e a vigilância em massa das telecomunicações são apenas alguns dos vários desafios à sociedade civil nicaraguense, que deve superar obstáculos cada vez mais complexos.

Em fevereiro de 2023, o governo Ortega implementou a decisão sem precedentes de retirar a nacionalidade nicaraguense de mais de 300 pessoas críticas ao seu mandato, fato amplamente repudiado pelas organizações de defesa dos direitos humanos (Yuhas, 2023). Em janeiro de 2024 se estabeleceu um enquadramento legal para essa ação, quando a Assembleia Nacional daquele país aprovou uma reforma constitucional que permite a retirada da nacionalidade a cidadãos condenados pelo crime de traição (EFE, 2024). Em setembro, Ortega voltou a utilizar esse recurso após libertar mais de uma centena de opositores e expulsá-los para a fronteira com a Guatemala (EFE, 2024).

3.8 VENEZUELA

Num ano eleitoral para a Venezuela, o primeiro semestre de 2024 foi como um preâmbulo do que finalmente aconteceu em julho e agosto (Conselho de Direitos Humanos das Nações Unidas, 2024). O diagnóstico da Venezuela para este relatório é limitado pelos seus próprios fatores metodológicos que estabelecem uma janela temporal (dezembro de 2023 a maio de 2024) que impede o aprofundamento dos acontecimentos após a amplamente questionada reeleição de Nicolás Maduro (The Carter Center, 2024). e o seu subsequente processo de repressão política em resposta ao protesto social. Assim, o relatório de contexto para a Venezuela neste documento pode ser considerado como uma análise das políticas e decisões que prepararam o caminho para as eleições.

O Relatório sobre a situação dos direitos humanos digitais na Venezuela 2022+2023, de VE sin Filtro, já alertava para a existência de um aparelho estatal "massivo" de intercepção de telecomunicações e de práticas arbitrárias por parte das autoridades, como exigir acesso a dados pessoais e conversas por meio de confisco de dispositivos (VE sin Filtro, 2023). O relatório menciona uma utilização abusiva de monitoramento nas redes sociais, normalmente dirigida a jornalistas e ativistas, e a sua utilização para realizar intimidações, ameaças e difundir discursos estigmatizantes contra a dissidência política. Também investiga o problema da conectividade fraca e precária que o venezuelano médio tem, que também é constantemente afetada por cortes de energia recorrentes em todo o país.

O relatório anual sobre direitos digitais de 2023, Algoritmos do Silêncio, mostrou um número de 128 violações de direitos humanos no ciberespaço dirigidas a jornalistas, cidadãos e organizações da sociedade civil (Instituto Prensa y Sociedad, 2023). O documento indica ainda que, durante aquele ano, 46 meios de comunicação independentes permaneceram bloqueados pelos provedores de internet que operam no país. Alguns desses novos bloqueios foram denunciados poucos meses antes das eleições, como é o caso dos portais El Político, Impacto e La Gran Aldea (Espacio Público, 2024).

Em fevereiro de 2024, a Digitel, uma das maiores companhias telefônicas do país, sofreu um ataque de ransomware que colocou em risco os dados pessoais de milhares de usuários e revelou a fraca infraestrutura com a qual trabalham várias das principais empresas do país (@vesinfiltro, 2024).

Em abril, o partido no poder promoveu um projeto denominado “Lei contra o fascismo, o neofascismo e expressões semelhantes”, que inclui uma definição muito aberta de comportamentos que considera “fascistas” e expõe as pessoas a penas de prisão por eles, o que segundo as organizações não governamentais, poderia ter um efeito limitante sobre a liberdade de expressão no país (Programa Venezuelano de Ação Educacional para os Direitos Humanos, 2024).

Em maio, o atual Ministro das Relações Exteriores da Venezuela, Diosdado Cabello, anunciou em seu programa de televisão a introdução de um projeto de lei que visa limitar a chegada de fundos do exterior para organizações da sociedade civil (Con el Mazo Dando, 2024). A possibilidade de incluir legislação desse tipo no ordenamento jurídico venezuelano já havia sido considerada em 2022 e 2023 (Calderón, 2024). Finalmente, dias após a reeleição de Maduro, a lei foi aprovada por maioria na Assembleia Nacional (Anistia Internacional, 2024).

4. ÁREAS TEMÁTICAS E ESTUDOS DE CASO

Esta seção contém a categorização de uma série de sistematizações de informações de diferentes fontes. Algumas dessas esquematizações baseiam-se em dados e outras têm a ver com experiências comuns que foram discutidas e padrões que foram identificados organicamente durante as diferentes reuniões organizadas pelo Observatório.

O capítulo pretende aprofundar e esclarecer cada um dos quatro eixos temáticos que o Observatório conseguiu identificar na sua articulação com as diferentes organizações: violência de gênero em espaços digitais, ataques a infraestruturas, vigilância e espionagem, e violações da liberdade de expressão online.

Conforme mencionado anteriormente, os dados recolhidos para a elaboração deste relatório foram coletados em três etapas: um primeiro período de dezembro de 2023 a janeiro de 2024 que coletou 163 casos; outra de fevereiro a março de 2024, com 135; e uma última de abril a maio de 2024, com 113 casos.

4.1 VIOLÊNCIA DIGITAL DE GÊNERO

As diferentes formas de expressão online da violência de género têm sido um eixo quase transversal no trabalho da maioria das organizações que fazem parte do OLAD. Por essa razão, e devido ao número de casos atendidos, o Observatório conseguiu realizar uma coleta de dados que permite um exercício mais aprofundado.

As organizações que fazem parte do OLAD e que trataram de casos de violência de gênero no espaço digital durante os respectivos períodos deste relatório foram Derechos Digitales (regional), Fundación Acceso (regional), Fundación Internet Bolivia (Bolívia), La Libre (Equador), MariaLab (Brasil), SocialTIC (México) e Taller de Comunicación Mujer (Equador).

Três dessas organizações gerem linhas diretas e oferecem apoio e resposta em casos de violência digital de gênero. As iniciativas atendem mulheres, crianças, ativistas, grupos de defesa dos direitos humanos e pessoas que fazem parte da comunidade LGTBQIA+. Esses projetos são: o Centro Digital SOS da Fundação InternetBolivia.org (Bolívia), Maria d'Ajuda do Marialab (Brasil) e Navegando Libres da Red de Taller Comunicación Mujer (Equador). Sobre esta matéria está também disponível o relatório *Linhas de apoio para abordar casos de violência de gênero em ambientes digitais: monitoramento e tendências na Bolívia, Brasil e Equador* que investigam padrões comuns em relação à violência digital de gênero na região (Araújo et al., 2024).

Durante o primeiro período temporário estabelecido pelo Observatório — de dezembro de 2023 a janeiro de 2024 — as organizações reportaram um total de 28 casos atendidos. No segundo período — de fevereiro a março de 2024 — o número de casos analisados aumentou consideravelmente para 50, número que representa quase um terço de todos os casos notificados nas diferentes linhas de trabalho. Por fim, no terceiro período — de abril a maio de 2024 — foram registrados 40 casos.

Dentro deste fluxo de trabalho foi possível identificar alguns padrões comuns na natureza dos casos abordados principalmente por organizações que lutam contra a violência de género, razão pela qual foram divididos em grupos temáticos que foram apresentados de forma ampla, devido a que a caracterização de cada fenômeno pode variar de acordo com os critérios de cada organização. O primeiro corresponde a casos de assédio digital[3], que nos três períodos estudados totalizou 39 ocorrências. O segundo

3 No relatório Linhas de ajuda para atender casos de violência de gênero em ambientes digitais: monitoramento e tendências na Bolívia, Brasil e Equador, em que foi utilizada outra janela temporal de estudo, duas das organizações que fazem parte do OLAD (InternetBolivia.org e Red de Taller Comunicación Mujer) relataram que o assédio digital foi a segunda violência digital mais comumente relatada por suas linhas de ajuda.

grupo está incluído no problema da divulgação de conteúdo íntimo ou sexual sem o consentimento da pessoa envolvida[4]. Nos três períodos estudados, essa categorização atingiu um total de 33 casos. O terceiro grupo é formado por registros de violações de contas de plataformas sociais pertencentes a mulheres ou grupos de mulheres que se dedicam ao ativismo em suas diferentes facetas. Dentro destas facetas, embora não exclusivamente, o ativismo feminista está muito presente. A soma dos casos desse grupo, nos três períodos analisados, é de 24.

Em todas essas expressões de violência de gênero online, os dados registrados pelas organizações mostram que, na grande maioria, esses tipos de ataques são dirigidos a pessoas particulares e que também, na maioria dos casos, os agressores são normalmente pessoas particulares. No entanto, também é visível uma percentagem considerável de casos em que o agressor não pôde ser identificado.

4.2 ATAQUES À INFRAESTRUTURA

Outra área de interesse do Observatório são as violações de sites e infraestruturas críticas para organizações de defesa dos direitos humanos, no seu mais amplo espectro. Nos prazos estabelecidos para a elaboração do relatório, mais de cinquenta casos foram atendidos pelas organizações que compõem o OLAD.

A grande maioria dos casos considerados neste relatório foram relatados por La Libre, uma pequena organização sediada no Equador que procura fornecer infraestrutura tecnológica "sólida e acessível" a organizações, pessoas e movimentos sociais que trabalham em defesa dos direitos humanos, da natureza, da justiça e da igualdade. Entre dezembro de 2023 e maio de 2024, La Libre recebeu pelo menos 34 casos relacionados a ataques a sites de organizações sociais e ativistas. Também tratou de 22 casos de ransomware ou sequestro de dados.

4 Esse tipo de caso está incluído na caracterização da violência sexual digital feita pela linha de ajuda Navegando Livremente pela Red de Taller de Comunicación Mujer [Rede de Oficina Comunicação Mulher], que no relatório Linhas de ajuda para atender casos de violência de gênero em ambientes digitais: monitoramento e tendências na Bolívia, Brasil e Equador são identificados como o tipo de violência digital mais atendido pela organização. No caso de Maria d'Ajuda do Marialab, esse comportamento se caracteriza como exposição de imagens íntimas e é o terceiro tipo de violência mais atendido por essa linha. Por outro lado, o Centro SOS Digital da Fundação InternetBolivia.org, no mesmo relatório, inclui este problema na categoria de abuso sexual por meio das Tecnologias de Informação (TIC), que inclui diversas formas de violência como ameaças e extorsão de vítimas relacionado à potencial publicação de conteúdo íntimo.

A disparidade nos dados relatados nesta seção se deve principalmente ao fato de que parte fundamental do trabalho do La Libre é, justamente, ajudar na construção e manutenção de infraestrutura, bem como oferecer suporte técnico às organizações.

La Libre está presente em vários países, embora atue principalmente no Equador. O seu cofundador, Jonathan Finlay, garante no relatório *Na mira* que a organização trabalha há 10 anos "desenvolvendo infraestruturas autónomas, implementando serviços, fornecendo soluções tecnológicas dirigidas aos defensores dos direitos humanos e da natureza".

A abordagem de La Libre é "orientada para o acompanhamento", tecendo redes com outras organizações sociais "para fortalecer as lutas". "Em alguns casos (as organizações) nos procuram porque estão sofrendo ou sofreram um ataque, porque perderam e querem recuperar informações, ou aplicativos, sites, redes. Ou, simplesmente, a sua organização necessita de melhorar a infraestrutura física das suas telecomunicações, ou uma reformulação do website", afirma Finlay.

Ou seja, La Libre oferece uma ampla gama de serviços digitais pensados especialmente para as necessidades de organizações e pessoas defensoras de direitos. A principal diferença com os serviços comerciais comuns é que "as pessoas que trabalham com direitos humanos geralmente estão em condições que não são as mesmas de uma empresa ou de um banco", explica. Por essa razão, as organizações "querem trabalhar com alguém que entenda o que está fazendo". A ideia é dar "apoio próximo", algo que não tem necessariamente a ver com aspectos técnicos.

Nem toda abordagem às ameaças digitais se refere apenas à parte técnica. Em casos de ransomware, por exemplo, quando a criptografia de um sistema é concluída, o foco está mais no "suporte e recomendações, primeiro para que isso não aconteça novamente, e segundo para que possam recuperar o máximo de informações possível no menor tempo".

No final de 2023, "houve um momento em várias organizações que, por diferentes meios e com diferentes programas de malware, dispositivos acabaram sendo infetados" em ataques de ransomware quase simultâneos. Foram afetados principalmente laptops e desktops, mas a organização também registrou dois casos de infecção de servidores. Finlay aponta que os ataques ocorreram no âmbito de "campanhas de

grupos deameaças" que enviavam e-mails do tipo phishing[5] direcionado às áreas administrativas das organizações e acabou infectando os computadores.

Outros tipos de casos, como ataques a websites, podem ser abordados de forma reativa. Normalmente são "ataques de negação de serviço"[6], adivinhação de senhas por meio de força bruta, infecção de sites por malware" ou casos em que técnicas de phishing foram usadas "para obter credenciais de sites e assumir controle temporário".

Quando chegam casos desse tipo, La Libre faz uma avaliação do caso "dependendo de cada cenário". Dependendo da natureza do ataque, as soluções técnicas podem ser simples ou, em casos mais complexos, recuperar o controle sobre uma página na internet ou rede pode ser um processo longo e complicado.

4.3 VIGILÂNCIA E ESPIONAGEM

Os casos do México e de El Salvador, descritos no capítulo sobre contexto regional, mostram a gravidade dos casos em que o uso de tecnologias de espionagem, supostamente fabricadas para exercer o domínio da lei, foi utilizado para objetivos políticos ou pessoais daqueles que possuem a capacidade de usar o monopólio da força do Estado.

O caso de El Salvador com o Pegasus é um pouco mais recente que o do México, onde os primeiros relatos do uso do Pegasus datam de 2017 (BBC Mundo, 2017). No entanto, a magnitude da sua utilização não foi revelada até a publicação de um projeto jornalístico transnacional em 2021 que revelou uma série de interceptações de centenas de personalidades entre jornalistas, ativistas e funcionários governamentais em todo o mundo (Forbidden Stories, 2021).

Somente no México o governo de Enrique Peña Nieto utilizou spyware[7] contra 15 mil

5 hishing: Técnica maliciosa de engenharia social que consiste no envio de e-mails, mensagens de texto, chamadas ou sites fraudulentos para enganar o usuário e induzi-lo a compartilhar seus dados pessoais, suas credenciais de acesso a uma plataforma ou forçá-lo a baixar algum tipo de malware em seu dispositivo (Kosinski , 2024).

6 Ataque de negação de serviço: Tipo de ataque cibernético malicioso que consiste na interrupção de um serviço. Normalmente funciona sobrecarregando solicitações em um site, por exemplo, causando uma interrupção quando o servidor recebe mais solicitações do que pode processar de uma vez (Cloudfare, n.d.).

7 Spyware: Software desenvolvido para coletar dados confidenciais de um dispositivo sem o consentimento de seu proprietário. O spyware geralmente é instalado em um dispositivo por meio de fraudes (Kaspersky, n.d.).

pessoas, incluindo familiares das vítimas do massacre de Ayotzinapa em 2014 (Romero, 2021). Nesse país, uma organização membro do OLAD trabalha há anos em questões de espionagem estatal: SocialTIC. Em abril de 2023, a organização publicou um relatório conjunto com o Centro Prodh, R3D e Artigo-19 que revelou evidências de novos casos de espionagem com Pegasus por parte do exército contra defensores de direitos humanos do Centro Prodh (Centro PRODH et al., 2023). Apenas um mês depois, o New York Times revelou outro caso importante segundo o qual o subsecretário de direitos humanos, Alejandro Encinas, foi interceptado (Kitroeff & Bergman, 2024).

No México, as organizações seguem um fluxo de trabalho coordenado para resolver casos de vigilância ilegal com o Pegasus. Através de uma aliança chamada Coalizão de Direitos Digitais composta por SocialTIC, R3D, Centro Prodh e Artigo 19. Assim, "cada organização tem um papel muito conciso" quando surge um caso, afirma Paúl Aguilar, coordenador de segurança digital da SocialTIC.

A R3D é responsável pela representação legal da vítima, a Artigo 19 documenta as violações da liberdade de expressão e o Centro Prodh documenta as violações dos direitos humanos que podem surgir em cada caso. A SocialTIC, por sua vez, se encarrega da parte técnica: análise dos dispositivos e demais ações. Essa tarefa é frequentemente realizada em colaboração com o CitizenLab da Universidade de Toronto.

Mas o trabalho da SocialTIC não se limita apenas à detecção de spyware. A organização também implementa uma série de capacitações com as vítimas "para ajudá-las a configurar os seus dispositivos" e a tomar as medidas necessárias para que uma situação semelhante "não se repita" ou, pelo menos, "torne mais difícil para o agressor".

A SocialTIC provê "atenção permanente às pessoas que poderiam ou foram monitoradas" por qualquer meio. Fazem-no individualmente e "especialmente com jornalistas que foram espionados" anteriormente e para os quais existem novas suspeitas de intervenção. "Isso mostra que estamos vendo uma reincidência nos casos", diz Aguilar. Em alguns casos é Pegasus, mas outros "têm a ver com indícios de outras tecnologias que aparentemente estão sendo utilizadas" no México. Mas não se trata apenas de spyware, mas também de interceptação de comunicações, monitoramento invasivo nas redes sociais, monitoramento físico e até campanhas de assédio nas redes. "É uma ação de vigilância e espionagem muito mais ampla, não focada apenas em spyware", afirma Aguilar.

Por outro lado, a SocialTIC realiza trabalhos com organizações que acompanham grupos de pessoas que foram vigiadas. Esses acompanhamentos são "muito mais amplos, pois envolvem poder trabalhar com toda a organização", afirma. O México está organizado politicamente sob um sistema federal descentralizado, que confere aos estados que o compõem uma série de poderes que incluem sistemas de segurança próprios, em nível municipal e estadual. E embora o Pegasus seja vendido apenas aos governos centrais e às suas agências de defesa, a utilização de outras tecnologias de vigilância e espionagem nos estados está em seu auge.

"Existem outras tecnologias que os estados estão comprando, talvez de baixa escala. Portanto, parece que eles estão tendo acesso a outros tipos de spyware menos sofisticados, bem como a outras tecnologias de comunicação e rastreamento menos sofisticadas. Proporcional às suas capacidades económicas", afirma Aguilar e acrescenta que "há evidências de que quase todos os 32 estados adquiriram tecnologias deste tipo (...) "Estamos trabalhando para demonstrar como elas têm sido usadas contra a sociedade civil".

4.4 VIOLAÇÕES DA LIBERDADE DE EXPRESSÃO ONLINE

O último grande foco da observação do OLAD são as violações da liberdade de expressão online. Nessa área, as organizações que fazem parte do Observatório trataram um total de 92 casos de ataques à liberdade de expressão nos seus respectivos países.

Nesta categoria relataram atender casos Derechos Digitales, Marialab, SocialTIC, La Libre, Fundación Internet Bolivia e Sursiendo. Entre todas as organizações, foi realizada a recuperação de 34 contas de redes sociais. De dezembro de 2023 a janeiro de 2024 foram 19; de fevereiro a março de 2024, 9; e de abril a maio de 2024, 6. As recuperações de contas — que podem ser retiradas devido a ataques cibernéticos ou esforços de denúncia em massa — foram realizadas no Facebook, Instagram, X (antigo Twitter) e WhatsApp. Como caracterização geral, os perfis cujos casos são atendidos com prioridade tendem a ser pessoas ligadas à defesa de direitos, ao ativismo social e ambiental e à busca por justiça e igualdade.

Outro ângulo desse fenômeno pode ser observado através do registro de campanhas de calúnia e difamação, por vezes coordenadas. De dezembro de 2023 a janeiro de 2024, as organizações relataram 20 casos nesta categoria; entre fevereiro e março de 2024, 14; e de abril a maio de 2024 foram 24.

Nessa subcategoria, os números do La Libre voltam a se destacar, já que nos três períodos de tempo, a soma dos casos atendidos por todas as organizações é de 58. Desse total, 51 foram atendidos pelo La Libre, no Equador.

No capítulo sobre o contexto regional, foi mencionada a situação hostil que existe contra os defensores dos direitos humanos no Equador desde a declaração do conflito armado interno em janeiro de 2024. É vital ter em conta este contexto de estigmatização dos defensores dos direitos humanos ao mencionar os casos tratados por La Libre. Quando se trata de campanhas difamatórias, La Libre trabalha principalmente com aconselhamento às pessoas afetadas.

No início do ano, quando o presidente do Equador decretou guerra interna, "houve campanhas que pareciam organizadas por grandes equipes de pessoas muito próximas do governo que procuravam afetar organizações que pediam respeito aos direitos humanos". Várias organizações de defesa dos direitos humanos, como o Comitê Permanente para a Defesa dos Direitos Humanos, que oferece aconselhamento gratuito às vítimas de crimes estatais, foram sinalizadas por centenas de contas simultaneamente.

Uma busca no X, ex-Twitter (X, 2004), que vazou entre os dias 9 e 15 de janeiro, com as palavras chaves "defensores" e "delinquentes", produz centenas de resultados como este: "Excelente trabalho @ffaa (conta das Forças Armadas), e a esses bichas defensores de delinquentes têm que receber amor igual", diz um usuário comentando um vídeo de cidadão onde são vistos atos de tortura por parte dos militares. A palavra-chave "Rulay" também leva a essa tendência. É o nome de uma música atribuída a um grupo criminoso que acabou virando trilha sonora, como meme, de dezenas de vídeos de soldados realizando torturas.

Durante as primeiras semanas da declaração do conflito armado, "era evidente que havia agências estatais que dedicaram os seus esforços, especialmente equipes de comunicação e consultores, que se concentraram na realização destes ataques", sustenta. "Era super violento. E foi constante e permanente", denuncia.

Finlay lembra o caso de uma organização que trabalha com pessoas privadas de liberdade que foi inicialmente objeto de comentários estigmatizantes e violentos nas redes sociais. Pouco depois, os comentários se transformaram em ameaças, por meio de e-mails e ligações insistentes.

"Nesse caso particular, o que se fez foi um processo de acompanhamento no qual foram propostas estratégias de como bloquear, por saúde mental, essa interação." Nesse cenário, foram implementadas ações como aconselhamento sobre configurações para bloqueio e isolamento de conteúdos em redes sociais, desenho de protocolos em caso de ameaças, formação sobre bloqueio de chamadas etc. Finlay define tudo isso como "um acompanhamento em segurança digital".

Paralelamente ao trabalho nessas áreas, Karisma (Colômbia) e Conexión Segura (Venezuela) têm trabalhado em estreita colaboração e possuem vasta experiência na documentação e análise de censura de conteúdo, bloqueio de redes e falhas de internet em contextos de efervescência social e repressão.

Na Colômbia, Karisma acompanhou um caso perante o Tribunal Constitucional para aceder a informações públicas sobre uma interrupção generalizada da Internet em Cali, num dos dias mais intensos da greve nacional de 2021. Os acontecimentos nunca foram investigados pelo governo do então presidente Iván Duque (Karisma, 2023). Por esse motivo, juntamente com outras organizações de defesa da liberdade de expressão, Karisma entrou com um pedido ao tribunal para esclarecer a situação (Botero & Parra, 2022). O Tribunal não determinou se a suspensão geral do serviço estava ou não correlacionada com os protestos. Contudo, ressaltou que o Estado não cumpriu seu papel ao não ter iniciado as investigações para esclarecer os fatos naquele momento.

Em contextos onde a censura é mais direta, como é o caso da Venezuela, as iniciativas a favor da liberdade de navegação e expressão online devem incluir outras abordagens. A Conexión Segura busca promover e difundir ferramentas básicas de segurança, por meio da divulgação de material amigável que ensine as pessoas, por exemplo, como usar uma VPN para visualizar sites que podem estar bloqueados na Venezuela, como sites de notícias. Justamente para esse fim, este ano lançaram um aplicativo para dispositivos Android: Noticias sin filtro (Conexão Segura, 2024).

5. LIÇÕES APRENDIDAS

FORMAÇÃO DE UM OBSERVATÓRIO REGIONAL

Em mais de três anos de trabalho, num enorme esforço de articulação das organizações filiadas, em condições voláveis e com uma carga avassaladora no seu trabalho quotidiano, o OLAD conseguiu colocar sobre a mesa alguns dos traços comuns em torno do estado dos direitos humanos no espectro digital na América Latina. O trabalho conjunto permitiu estreitar os laços de confiança entre organizações muito diversas e com diferentes frentes de luta.

O resultado disso é um esforço interseccional coletivo para compreender, a partir de uma perspectiva regional, os aspectos-chave da defesa dos direitos online: ameaças à democracia ou à liberdade de imprensa e expressão, abusos do Estado e violência de gênero são só algumas das formas nas quais se pode ver a tecnologia sendo utilizada como elemento coercitivo por atores maliciosos.

A articulação de um conjunto dessas características tem sido um enorme desafio, assim como os processos de discussão que levaram à identificação de padrões comuns na região e que finalmente conduziram à redação deste relatório.

O maior desafio, no entanto, tem sido a implementação de um sistema que permita medir ou quantificar os resultados do trabalho conjunto entre as diferentes organizações, que neste relatório foi denominado “relatório de casos próprios”. É um processo que, tal como a formação do OLAD em anos anteriores, exige uma adaptação em tempo real às necessidades das organizações que o compõem.

A criação de um observatório regional para ameaças digitais é uma tarefa complexa e a coordenação do trabalho comum enquanto as agendas individuais de cada organização são desenvolvidas em paralelo representa um grande desafio que deverá ser analisado no próximo período de trabalho do Observatório. É importante notar que a ampla gama de características das organizações envolvidas torna a medição quantitativa mais complexa, por isso este relatório recomenda a adoção de modificações e adaptações metodológicas para superar esses obstáculos.

Ao mesmo tempo, existem aspectos da metodologia que devem ser replicados e que podem até ser ampliados com o propósito de recolher informação mais segmentada

que ajude a caracterizar os tipos de agressão, as vítimas, o perfil dos agressores e o tipo de tecnologias utilizadas para violar direitos. É o caso, por exemplo, dos dados produzidos por organizações dedicadas a abordar e atender a violência de gênero no espaço digital.

Portanto, entende-se que é uma necessidade para os próximos ciclos do OLAD identificar em quais áreas de estudo é apropriado adaptar processos qualitativos e em quais áreas, pelo contrário, é necessário aprofundar a medição quantitativa.

REFLEXÕES SOBRE O PERÍODO ANALISADO

Este relatório permite-nos concluir que alguns dos principais atores que ameaçam os defensores dos direitos humanos são governos, grupos antidireitos que ameaçam a liberdade de expressão online, criminosos que estão presentes no ciberespaço e indivíduos que, por meio de expressões de sexismo e racismo estrutural, afetam principalmente mulheres e pessoas LGBTQIA+. A ausência de respostas estatais é quase uma constante e um fator transversal na região. Também destaca uma tendência crescente de adoção de políticas e estratégias autoritárias por vários governos da região, o que acrescenta uma camada adicional de vulnerabilidade à população vitimizada.

No meio de uma onda de criminalidade nunca antes vista na região (Crisis Group, 2023), há uma presença crescente de atores criminosos envolvidos em violações de direitos no espectro digital. Um exemplo desse tipo de dinâmica é a utilização do sistema de geolocalização de uma agência estatal por um líder criminoso no Equador para monitorar o candidato presidencial assassinado Fernando Villavicencio. A ideia de que um grupo criminoso organizado possa ter acesso, em tempo real, a dados pessoais sensíveis de cidadãos levanta um alarme regional, uma vez que o que está ocorrendo no Equador pode já estar acontecendo em outros países.

Em termos de vigilância e espionagem, verifica-se uma tendência crescente na adoção de tecnologias desse tipo. Estas estão cada vez mais acessíveis, especialmente para os governos locais. No caso de spywares mais sofisticados como o Pegasus, também se observa um padrão regional quando, enquanto este relatório estava sendo escrito, o presidente colombiano Gustavo Petro verificava uma suposta compra irregular de spyware durante o governo de seu antecessor, Iván Duque (El Espectador, 2024).

A Colômbia se torna assim o quinto país latino-americano que registra o uso do software, junto com México, El Salvador, Panamá e República Dominicana. Este relatório recomenda a atualização da metodologia de trabalho nesta área, talvez em uma direção qualitativa, para encontrar mecanismos de medição do trabalho das organizações numa perspectiva regional.

Vários países da região, por outro lado, enfrentam grandes desafios com a desinformação eleitoral e política. O Brasil, por exemplo, está tentando introduzir discussões sobre o papel das plataformas sociais na democracia, tendo como prioridade abordar a questão da desinformação. O Estado brasileiro tem enfrentado o poderoso lobby das grandes empresas de tecnologia nesse caminho. Na Bolívia, sob extrema polarização como resultado da dissolução do seu partido no poder, a desinformação está ganhando terreno com mais força entre as populações indígenas rurais. Na Colômbia, a luta contra a desinformação tem sido terreno fértil para inúmeras propostas legislativas, nenhuma aprovada até agora, que incluem perigosamente mecanismos de censura e colocam em risco o ecossistema digital.

Tal como o impacto em infraestruturas críticas, como um oleoduto ou um banco, as ameaças cibernéticas enfrentadas por pessoas, comunidades e organizações que defendem os direitos humanos e a natureza representam uma violação grave dos seus direitos. Esse tipo de ataques deixa não só um impacto pessoal, mas também coletivo, uma vez que representam um ataque às raízes da ordem democrática dos seus países. A visão do OLAD baseia-se nesse preceito, que busca dar uma resposta latino-americana de resiliência aos violentos fenômenos digitais que afligem sua população, recebida de diversas frentes.

6.REFERÊNCIAS

Abrão, C. (2024, junio 6). Corte Suprema de Brasil firma acuerdo con principales plataformas de redes sociales para combatir la desinforma. Gazeta do Povo. https://agenciabrasil.ebc.com.br/justica/noticia/2024-06/stf-assina-acordo-com-redes-sociais-para-combater-desinformacao

AFP. (2024, marzo 4). TikTok, nueva herramienta de reclutamiento guerrillero en Colombia. RFI. https://www.rfi.fr/es/m%C3%A1s-noticias/20240403-tiktok-nueva-herramienta-de-reclutamiento-guerrillero-en-colombia

Ameno, F. (2024, diciembre 3). Farra com dados: Uso de ferramenta que cruza conexões do Facebook e dados da polícia explode no país. Intercept Brasil. https://www.intercept.com.br/2024/03/12/uso-de-ferramenta-que-cruza-conexoes-do-facebook-e-dados-da-policia-explode-no-pais/

Amnistía Internacional. (2024a, agosto 16). Venezuela: Aprobación de Ley anti-ONG castiga la asistencia a víctimas y la defensa de los derechos humanos. Amnistía Internacional. https://www.amnesty.org/es/latest/news/2024/08/venezuela-aprobacion-ley-anti-ong-castiga-asistencia-victimas-defensa-derechos-humanos/

Amnistía Internacional. (2024b, septiembre 24). Colectivos y movimientos al frente de la defensa de derechos humanos en Guayaquil y la costa de Ecuador. Amnistía Internacional. https://www.amnesty.org/es/latest/campaigns/2024/09/colectivos-y-movimientos-al-frente-de-la-defensa-de-derechos-humanos-en-guayaquil-y-la-costa-de-ecuador/

Araújo, D., Mendez, L. A., Osorio, M., Diego, M., Priscilla, P., Venturini, J., & Lobato, C. (2024, noviembre). Líneas de ayuda para atender casos de violencia de género en entornos digitales: Monitoreo y tendencias en Bolivia, Brasil y Ecuador. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/LineasAyuda-ESP.pdf

Artículo 19. (2024, junio 2). SCJN confirma que Hacienda deberá entregar información relativa al caso Pegasus. Article 19 MX-CA. https://articulo19.org/scjn-confirma-que-hacienda-debera-entregar-informacion-relativa-al-caso-pegasus/

Asamblea Nacional del Ecuador. (2024, junio 6). Asamblea Nacional archivó el proyecto de Ley de Seguridad Digital. https://www.asambleanacional.gob.ec/es/noticia/96846-asamblea-nacional-archivo-el-proyecto-de-ley-de

BBC Mundo. (2017, junio 20). Cómo protegerte de Pegasus, el sistema de vigilancia en el centro de las acusaciones de espionaje a periodistas en México. BBC Mundo. https://www.bbc.com/mundo/noticias-40341302

BBC Mundo. (2023, julio 10). Matan en una cárcel de Ecuador a 7 ciudadanos colombianos acusados por el asesinato del candidato presidencial Fernando Villavicencio. BBC Mundo. https://www.bbc.com/mundo/articles/c3gx53lezgjo

BBC News Brasil. (2024, noviembre 25). O que é o FirstMile, software que teria sido usado pela Abin para monitorar jornalistas e ministros do STF. BBC News Brasil. https://www.bbc.com/portuguese/articles/c3g32mz1dzdo

BBC News Mundo. (2024a, abril 16). Twitter vs Elon Musk: Qué es la píldora venenosa con la que la red social quiere evitar la compra hostil del empresario. BBC News Mundo. https://www.bbc.com/mundo/noticias-61124066

BBC News Mundo. (2024b, mayo 10). Quién era Leandro Norero, el patrón, uno de los principales narcos de Ecuador que murió asesinado en la última matanza carcelaria en el país. BBC News Mundo. https://www.bbc.com/mundo/noticias-america-latina-63139767

BBC News Mundo. (2024c, junio 26). Cómo fue el intento de golpe de Estado que denunció el presidente de Bolivia después de que militares tomaran el centro de La Paz y entraran en la antigua sede de gobierno. BBC News Mundo. https://www.bbc.com/mundo/articles/c2jj33v45m7o

BBC News Mundo. (2024d, agosto 1). Cómo ocurrió el asalto de miles de seguidores de Bolsonaro a las sedes de los tres poderes en Brasil. BBC News Mundo. https://www.bbc.com/mundo/noticias-america-latina-64205936

BBC News Mundo. (2024e, agosto 30). 5 preguntas para entender por qué un juez en Brasil ordenó el bloqueo de la red social X en todo el país. BBC News Mundo. https://www.bbc.com/mundo/articles/c0rwjll15yqo

BBC News Mundo. (2024f, septiembre 1). El presidente Daniel Noboa declara la existencia de un conflicto armado interno en Ecuador y ordena al Ejército restablecer el orden tras varios atentados y la toma de un canal de TV. BBC News Mundo. https://www.bbc.com/mundo/articles/c3gy2zz03dpo

Belson, D. (2023, diciembre 12). Cloudflare 2023 Year in Review. The Cloudfare Blog. https://blog.cloudflare.com/radar-2023-year-in-review/

Beltrán, D. (2024, octubre 24). Gustavo Petro insistió en señalar al Gobierno Duque por la compra de Pegasus: Engañaron al estado de Israel, a la justicia y a Colombia. Infobae. https://www.infobae.com/colombia/2024/10/24/gustavo-petro-insistio-en-sus-criticas-por-la-compra-de-pegasus-enganaron-al-estado-de-israel-enganaron-la-justicia-colombiana-y-enganaron-a-colombia/

Bernal, A. (2024, agosto 3). Las políticas de Bukele: Una amenaza directa a la democracia. Open Democracy. https://www.opendemocracy.net/es/politicas-bukele-amenaza-democracia/

Biller, D., & Sá Pessoa, G. (2024, agosto 4). Elon Musk will be investigated over fake news and obstruction in Brazil after a Supreme Court order. AP. https://apnews.com/article/brazil-musk-x-supreme-court-investigation-a645757b95a66ee658832802908466ab

Bonifaz, R. (2024, febrero 25). Las fisuras de los sistemas de vigilancia en Ecuador. La Barra Espaciadora. https://www.labarraespaciadora.com/editorial/las-fisuras-sistemas-vigilancia-ecuador/

Bonifaz, R., & Silva, I. (2024, abril 26). Ola Bini y la criminalización del conocimiento. Derechos Digitales. https://www.derechosdigitales.org/23597/ola-bini-y-la-criminalizacion-del-conocimiento/

Botero, C., & Parra, J. (2022, octubre 24). El misterio detrás de los cortes de internet en cali durante el paro de 2021. Karisma. https://web.karisma.org.co/el-misterio-detras-de-los-cortes-de-internet-en-cali-durante-el-paro-de-2021/

Calderón, D. (2024, mayo 31). Una propuesta de ley contra el activismo. Derechos Digitales. https://www.derechosdigitales.org/23810/una-propuesta-de-ley-contra-el-activismo/

Câmara dos Deputados. (2024, abril 3). Conselho debate remuneração de conteúdo jornalístico nas plataformas digitais. Câmara dos Deputados. https://www.camara.leg.br/noticias/1039447-conselho-debate-remuneracao-de-conteudo-jornalistico-nas-plataformas-digitais/

Cañizares, A., Alvarado, A., John, T., Rios, M., & AnneClaire, S. (2024, octubre 1). Qué está pasando en Ecuador tras los hechos de violencia que sacuden el país. CNN en Español. https://cnnespanol.cnn.com/2024/01/10/ecuador-violencia-conflicto-armado-estado-excepcion-recap-trax

Carrillo, P. (2024, junio 20). La seguridad digital se hunde en el pantano político. La Barra Espaciadora. https://www.labarraespaciadora.com/ciberespacio/la-seguridad-digital-se-hunde-en-el-pantano-politico/

Castañeda, A. (2022, noviembre 8). Por medio del cual se adoptan medidas de prevención, protección, reparación y penalización de la violencia de género digital y se dictan otras disposiciones. Congreso de la República de Colombia. https://www.camara.gov.co/violencia-digital-de-genero

@cdh.gye. (2024, septiembre 2). CDH Bajo ataque [Post]. Instagram. https://www.instagram.com/p/C3JCcRrOagO/?igsh=dDRod3RkMXNoYjUz

Centro PRODH, R3D, SocialTIC, & ARTICLE 19. (2023, abril). Centro PRODH nuevamente atacado con Pegasus: Cómo la impunidad y la militarización proporcionaron la repetición del espionaje. https://socialtic.org/wp-content/uploads/2023/04/EE_Colibri_final.pdf

Chambers, B. (2022, octubre 21). Tribunal Superior Electoral de Brasil toma medidas contra la desinformación previo a la segunda vuelta presidencial. Agencia Anadolu. https://www.aa.com.tr/es/mundo/tribunal-superior-electoral-de-brasil-toma-medidas-contra-la-desinformaci%C3%B3n-previo-a-la-segunda-vuelta-presidencial/2717000

ChequeaBolivia. (2024, mayo 30). El impacto de la desinformación y los desafíos del periodismo en regiones clave de Bolivia. ChequeaBolivia. https://chequeabolivia.bo/el-impacto-de-la-desinformacion-y-los-desafios-del-periodismo-en-regiones-clave-de-bolivia

Cloudfare. (s/f). ¿Qué es un ataque de denegación de servicio (DoS)? Cloudfare. https://www.cloudflare.com/es-es/learning/ddos/glossary/denial-of-service/

CNN Español. (2024a, enero 29). ¿Por qué puede Bukele ser candidato en las elecciones presidenciales de El Salvador en 2024? CNN en Español. https://cnnespanol.cnn.com/2024/01/29/bukele-reeleccion-el-salvador-orix

CNN Español. (2024b, mayo 4). Revocan sentencia de inocencia a Ola Bini, amigo de Julian Assange, y lo declaran culpable de acceso ilegal a sistema informático. CNN en Español. https://cnnespanol.cnn.com/2024/04/05/ola-bini-assange-culpable-ecuador-orix

Coalizão Direitos Na Rede. (2024, agosto 7). Defendiendo la legislación brasileña sobre IA que protege los derechos. Coalizão Direitos Na Rede. https://direitosnarede.org.br/2024/07/08/defendiendo-la-legislacion-brasilena-sobre-ia-que-protege-los-derechos/

Colombo, G. (2024, marzo 23). Lobby de big techs trava enfrentamento às fake news, dizem advogados. Poder 360. https://www.poder360.com.br/brasil/big-techs-sao-desafio-para-tse-conter-fake-news-nas-eleicoes/?ref=nucleo.jor.br

Comisión Interamericana de Derechos Humanos. (2018, junio 21). Graves violaciones a los derechos humanos en el marco de las protestas sociales en Nicaragua. Comisión Interamericana de Derechos Humanos. https://www.oas.org/es/cidh/informes/pdfs/Nicaragua2018-es.pdf

Con el Mazo Dando. (2024, mayo 20). Cabello sobre Ley de Fiscalización de las ONG: Van a tener que explicar de dónde vienen los fondos. Con el Mazo Dando. https://mazo4f.com/cabello-sobre-ley-de-fiscalizacion-de-las-ong-van-a-tener-que-explicar-de-donde-vienen-los-fondos

Conexión Segura. (2024). Noticias Sin Filtro. https://noticiassinfiltro.com/

Congreso de la República de Colombia. (s/f). Gacetas del Congreso de la República de Colombia [Dataset]. Gacetas del Congreso. Recuperado el 12 de abril de 2024, de http://svrpubindc.imprenta.gov.co/senado/index.xhtml

Consejo de Derechos Humanos de las Naciones Unidas. (2024, octubre 15). La Misión Internacional de la ONU revela graves violaciones de derechos humanos en Venezuela durante el período electoral 2024. Consejo de Derechos Humanos

de las Naciones Unidas. https://www.ohchr.org/es/press-releases/2024/10/un-international-mission-reveals-gross-human-rights-violations-venezuela

Crisis Group. (2023, diciembre 5). América Latina lucha contra una nueva ola de criminalidad. Crisis Group. https://www.crisisgroup.org/es/latin-america-caribbean/latin-america-wrestles-new-crime-wave

Curipoma, L. (2024, noviembre 4). El perverso goce ante la violación de derechos humanos en detenciones militares. INREDH. https://inredh.org/el-perverso-goce-ante-la-violacion-de-derechos-humanos-en-detenciones-militares/

Derechos Digitales. (2022, noviembre 2). Las reformas legales en El Salvador: Un gran retroceso en los derechos humanos y el Estado democrático. Derechos Digitales. https://www.derechosdigitales.org/17840/las-reformas-legales-en-el-salvador-un-gran-retroceso-en-los-derechos-humanos-y-el-estado-democratico/

Derechos Digitales. (2023, septiembre). Derechos humanos en entornos digitales en Nicaragua. Derechos Digitales. https://www.derechosdigitales.org/publicaciones/derechos-humanos-en-entornos-digitales-en-nicaragua/.

Díaz, V. (2022, enero 4). Voto electrónico y consideraciones de política pública en América Latina. Derechos Digitales América Latina. https://www.derechosdigitales.org/wp-content/uploads/VotoElectronico-mapalatino.pdf

Do Alto, H. (2007). El MAS-IPSP boliviano, entre movimiento social y partido político. Análisis Político, 62, 26. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-47052008000100002

DW. (2024, agosto 4). Brasil: Elon Musk exige la renuncia de Alexandre de Moraes. DW. https://www.dw.com/es/brasil-elon-musk-exige-la-renuncia-de-alexandre-de-moraes/a-68763337

ECU-911. (s/f-a). Cámaras de Videovigilancia. ECU-911. Recuperado el 29 de noviembre de 2024, de https://www.ecu911.gob.ec/camaras-de-videovigilancia/

ECU-911. (s/f-b). Localizador Móvil. ECU-911. Recuperado el 29 de noviembre de 2024, de https://www.ecu911.gob.ec/localizador-mobil/

EFE. (2023, diciembre 19). El Gobierno brasileño lanza una aplicación para bloquear teléfonos celulares robados. Swissinfo. https://www.swissinfo.ch/spa/el-gobierno-brasile%C3%B1o-lanza-una-aplicaci%C3%B3n-para-bloquear-tel%C3%A9fonos-celulares-robados/49073140

EFE. (2024a, enero 19). El régimen de Nicaragua ratificó una reforma que despoja de la nacionalidad a los condenados por traición a la patria. Infobae. https://www.infobae.com/america/america-latina/2024/01/20/el-regimen-de-nicaragua-ratifico-una-reforma-que-despoja-de-la-nacionalidad-a-los-condenados-por-traicion-a-la-patria/

EFE. (2024b, octubre 9). Nicaragua despoja de su nacionalidad a 135 exdetenidos que expulsó hacia Guatemala. France24. https://www.france24.com/es/am%C3%A9rica-latina/20240910-o-nicaragua-despoja-de-su-nacionalidad-a-135-presos-pol%C3%ADticos-que-expuls%C3%B3-hacia-guatemala

El Espectador. (2024, octubre 22). El dueño de Pegasus ha lavado activos en Colombia: Presidente Petro. El Espectador.https://www.elespectador.com/politica/pegasus-petro-dijo-que-el-dueno-del-software-gerente-de-nso-group-lavo-activos-en-colombia-vuelos-noticias-hoy/

El Universo. (2023, diciembre 12). Contraloría empieza auditorías a los contratos del Consejo Nacional Electoral para hacer las elecciones presidenciales anticipadas. El Universo. https://www.eluniverso.com/noticias/politica/contraloria-general-del-estado-consejo-nacional-electoral-voto-telematico-contratos-fallas-auditorias-elecciones-presidenciales-2023-nota/

Electronic Frontier Foundation. (2021, junio 28). Carta de la EFF a la Secretaría de Derechos Humanos de la República de Ecuador (caso Ola Bini). Electronic Frontier Foundation. https://www.eff.org/document/carta-de-la-eff-la-secretaria-de-derechos-humanos-de-la-republica-de-ecuador-caso-ola-bini

ESET. (s/f). Ransomware. ESET. Recuperado el 29 de noviembre de 2024, de https://www.eset.com/es/caracteristicas/ransomware/

Espacio Público. (2024a, mayo 20). Operadoras bloquean portal web del medio digital La Gran Aldea. Espacio Público. https://espaciopublico.ong/operadoras-bloquean-portal-web-del-medio-digital-la-gran-aldea/

Espacio Público. (2024b, junio 3). Operadoras de internet bloquean portal informativo El Político. Espacio Público. https://espaciopublico.ong/operadoras-de-internet-bloquean-portal-informativo-el-politico/

Espacio Público. (2024c, septiembre 3). Bloquean portal web del medio Impacto Venezuela. Espacio Público. https://espaciopublico.ong/bloquean-portal-web-del-medio-impacto-venezuela/

Falcão, M. (2024, enero 31). PF vê abuso de poder econômico e manipulação de dados em campanha de Google e Telegram contra PL das Fake News. Globo. https://g1.globo.com/politica/noticia/2024/01/31/pf-ve-abuso-de-poder-economico-e-manipulacao-de-dados-em-campanha-do-google-e-telegram-contra-pl-das-fake-news.ghtml

Fiscalía General del Estado Ecuador. (2024). Caso Metástasis. Fiscalía General del Estado Ecuador. https://www.fiscalia.gob.ec/caso-metastasis/

Folha de Sao Paulo. (2024, noviembre 29). Moraes inclui Musk em inquérito das milícias digitais e abre nova investigação sobre obstrução. Folha de Sao Paulo. https://www1.folha.uol.com.br/poder/2024/04/moraes-inclui-musk-como-investigado-no-inquerito-das-milicias-digitais.shtml

Forbidden Stories. (2021). Pegasus Project. Forbidden Stories. https://forbiddenstories.org/projects_posts/pegasus-project/

Fundamedios. (2024, febrero 21). Indómita recibe un nuevo ataque cibernético, van 300 desde diciembre [Post]. https://www.fundamedios.org.ec/alertas/indomita-recibe-un-nuevo-ataque-cibernetico-van-300-desde-diciembre/

Gavarrete, J., Reyes, D., & Martínez, Ó. (2022, diciembre 1). Veintidós miembros de El Faro fueron intervenidos con Pegasus 226 veces entre 2020 y 2021. El Faro. https://elfaro.net/es/202201/el_salvador/25935/Veintid%C3%B3s-miembros-de-El-Faro-fueron-intervenidos-con-Pegasus-226-veces-entre-2020-y-2021.htm

Global Freedoom Of Expression Columbia University. (2020, mayo 26). El caso de la investigación sobre las noticias falsas en Brasil. Columbia University. https://globalfreedomofexpression.columbia.edu/es/cases/the-case-of-the-brazil-fake-news-inquiry/

Gressier, R. (2024, julio 24). Gigantes de tecnología y prensa dan espaldarazo a la apelación de El Faro en caso Pegasus. El Faro. https://elfaro.net/es/202407/el_salvador/27511/Gigantes-de-tecnolog%C3%ADa-y-prensa-dan-espaldarazo-a-la-apelaci%C3%B3n-de-El-Faro-en-caso-Pegasus.htm

Human Rights Watch. (2024, mayo 22). Ecuador: Abusos luego del anuncio de un 'conflicto armado'. Human Rights Watch. https://www.hrw.org/es/news/2024/05/22/ecuador-abusos-luego-del-anuncio-de-un-conflicto-armado

Instituto Nacional de Estadística de Bolivia. (2024, marzo 23). Censo Bolivia 2024. Instituto Nacional de Estadística de Bolivia. https://censo.ine.gob.bo/

Instituto Prensa y Sociedad. (2023). Algoritmos del silencio: Reporte anual de Derechos Digitales 2023. Instituto Prensa y Sociedad. https://ipysvenezuela.org/wp-content/uploads/2024/05/IPYS_ReporteDerechosDigitales-2023.pdf

Karisma. (2023, octubre 14). ¿Cortaron o no cortaron el internet durante el Paro Nacional del 2021? Karisma. https://www.instagram.com/karismacol/reel/CyYv1rWOSf6/

Karisma. (2024, julio 6). Proyecto de ley ofrece nuevas formas de censura impuestas por funcionarios públicos mientras desprotege a víctimas de violencia de género. Karisma. https://web.karisma.org.co/proyecto-de-ley-ofrece-nuevas-formas-de-censura-impuestas-por-funcionarios-publicos-mientras-desprotege-a-victimas-de-violencia-de-genero/

Kaspersky. (s/f). Spyware: ¿Qué es y cómo protegerse? Kaspersky. Recuperado el 29 de noviembre de 2024, de https://latam.kaspersky.com/resource-center/threats/spyware?srsltid=AfmBOoqc5IIKjYFs65cr97NVgoZeJoGiZhFn-ovKTzhJlSDlM8IsuU-h

Kitroeff, N., & Bergman, R. (2024, mayo 22). El espionaje en México cobra una nueva víctima: Un aliado del presidente. The New York Times. https://www.nytimes.com/es/2023/05/22/espanol/alejandro-encinas-pegasus-espionaje.html

Knoerr, J. (2024, mayo 22). Investigadores observan un aumento de la desinformación a medida que los conflictos sociopolíticos afectan a las comunidades locales de Bolivia, El Salvador y Perú. LatAm Journalism Review. https://latamjournalismreview.org/es/articles/investigadores-observan-un-aumento-de-la-desinformacion-a-medida-que-los-conflictos-sociopoliticos-afectan-a-las-comunidades-locales-de-bolivia-el-salvador-y-peru/

Kosinski, M. (2024, mayo 17). ¿Qué es el phishing? IBM. https://www.ibm.com/es-es/topics/phishing#:~:text=El%20phishing%20es%20un%20tipo,otro%20modo%20a%20la%20ciberdelincuencia.

La Barra Espaciadora. (2024, octubre 13). Voto telemático y seguridad informática: Lo que nadie tomó en cuenta. La Barra Espaciadora. https://www.labarraespaciadora.com/ciberespacio/voto-telematico-seguridad-informatica/

Maia, P. (2023, agosto 1). A Cautionary Tale: Brazilian democracy, anti-democratic riots, and Meta's platforms. The Influence Industry Project. https://influenceindustry.org/en/explorer/case-studies/brazil-elections-meta-platforms/

Megiddo, G. (2024, mayo 26). $13m Cash on a Private Jet: How Colombia Paid for Israeli Spyware. Haaretz. https://www.haaretz.com/israel-news/2024-03-26/ty-article-magazine/.premium/13m-cash-on-a-private-jet-from-colombia-a-nonissue-for-israeli-head-of-defense-export/0000018e-7689-d706-a39f-f7f93fa10000

Ministerio TIC. (2024). Estrategia Nacional Digital de Colombia 2023 — 2026. Ministerio TIC. https://www.mintic.gov.co/portal/715/articles-334120_recurso_1.pdf

Molina, F. (2023, septiembre 28). Evo Morales y Luis Arce llevan al MAS al divorcio tras una larga pelea. El País. https://elpais.com/internacional/2023-09-28/evo-morales-y-luis-arce-llevan-al-mas-al-divorcio-tras-una-larga-pelea.html

Moreno, C. (2022, septiembre 27). Es tiempo de una ley sobre violencia digital de género. Karisma. https://web.karisma.org.co/es-tiempo-de-una-ley-sobre-violencia-digital-de-genero%EF%BF%BC/

Moreno, C. (2024, mayo 24). Un proyecto para proteger mujeres que protege es a políticos. La Silla Vacía. https://www.lasillavacia.com/red-de-expertos/red-de-las-mujeres/un-proyecto-para-proteger-mujeres-que-protege-es-a-politicos/

Observatorio Ecuatoriano de Crimen Organizado. (2024). Boletín anual de homicidios intencionales en Ecuador: Análisis de las estadísticas finales del año 2023. Observatorio Ecuatoriano de Crimen Organizado. https://oeco.padf.org/boletin-semestral-de-homicidios-intencionales-en-ecuador/

OEA. (2018, diciembre 19). CIDH denuncia agravamiento de la represión y el cierre de espacios democráticos en Nicaragua. OEA. https://www.oas.org/es/cidh/prensa/Comunicados/2018/273.asp

Osorio, M. (2024, septiembre 2). El riesgo constante de ser periodista en México: Un caso de filtración de datos personales. Derechos Digitales. https://www.derechosdigitales.org/23158/el-riesgo-constante-de-ser-periodista-en-mexico-un-caso-de-filtracion-de-datos-personales/

Primicias. (2024, noviembre 29). Caso Villavicencio: ECU-911 confirma el mal uso de la plataforma de rastreo de celulares. Primicias. https://www.primicias.ec/noticias/sucesos/ecu911-rastreo-celulares-caso-villavicencio/

Proceso. (2024, diciembre 1). Caso Pegasus: Absuelven al único acusado por el espionaje a Carmen Aristegui. Proceso. https://www.proceso.com.mx/nacional/2024/1/12/caso-pegasus-absuelven-al-unico-acusado-por-el-espionaje-carmen-aristegui-321992.html

Programa Venezolano de Educación Acción en Derechos Humanos. (2024, abril 4). Venezuela frente al espejo del fascismo: Perspectivas de derechos humanos sobre el proyecto Ley contra el fascismo, neofascismo y expresiones similares. Programa Venezolano de Educación Acción en Derechos Humanos. https://provea.org/actualidad/venezuela-frente-al-espejo-del-fascismo-perspectivas-de-derechos-humanos-sobre-el-proyecto-ley-contra-el-fascismo-neofascismo-y-expresiones-similares-laboratorio-de-paz/

Projeto de Lei n° 2338. (2023). Senado Federal. https://www25.senado.leg.br/web/atividade/materias/-/materia/157233

R3D. (2024a, febrero 27). Ejército de Bots: Las operaciones militares para monitorear las críticas en redes sociales y manipular la conversación digital. R3D. https://r3d.mx/2024/02/27/ejercito-de-bots-las-operaciones-militares-para-monitorear-las-criticas-en-redes-sociales-y-manipular-la-conversacion-digital/

R3D. (2024b, abril 24). Coppel guarda silencio sobre el incidente de ciberseguridad que afectó a sus sistemas. R3D. https://r3d.mx/2024/04/24/coppel-guarda-silencio-sobre-el-incidente-de-ciberseguridad-que-afecto-a-sus-sistemas/

Revista Semana. (2024, mayo 4). FF.MM. reaccionan a actuar de las disidencias al reclutar a menores a través de TikTok: Es una flagrante violación al mismo cese al fuego. Revista Semana. https://www.semana.com/nacion/articulo/ffmm-reaccionan-a-actuar-de-las-disidencias-al-reclutar-a-menores-a-traves-de-tiktok-es-una-flagrante-violacion-al-mismo-cese-al-fuego/202446/

Reyes, E. (2024, agosto 21). Ley de Ciberseguridad en México; una propuesta sin sustento técnico. Expansión. https://expansion.mx/tecnologia/2024/08/21/es-posible-una-ley-de-ciberseguridad-en-mexico

Rodríguez, M. (2024, enero 29). Salud Total EPS denunció ser víctima de ataque cibernético: Confirmó a sus usuarios si sus servicios se vieron afectados. Infobae. https://www.infobae.com/colombia/2024/01/30/salud-total-denuncio-ser-victima-de-ataque-cibernetico-eps-confirmo-a-sus-usuarios-si-sus-servicios-se-vieron-afectados/

Romero, M. (2021, julio 20). México: El Gobierno de Peña Nieto investigó a 15.000 personas con Pegasus. France24. https://www.france24.com/es/am%C3%A9rica-latina/20210720-pegasus-espionaje-mexico-pena-nieto

RSF. (2024a). Clasificación mundial de la libertad de prensa 2024: El periodismo, bajo las presiones políticas. RSF. https://rsf.org/es/clasificaci%C3%B3n-mundial-de-la-libertad-de-prensa-2024-el-periodismo-bajo-las-presiones-pol%C3%ADticas#:~:text=En%20la%20regi%C3%B3n%20Asia-Pac%C3%ADfico,)%20y%20Afganist%C3%A1n%20(178%C2%BA)

RSF. (2024b). El Salvador. RSF. https://rsf.org/en/country/el-salvador

Sadi, A. (2024, enero 25). Espionagem ilegal da Abin atingiu 30 mil pessoas e dados foram guardados em Israel, diz chefe da PF. Globo. https://g1.globo.com/politica/blog/andreia-sadi/post/2024/01/25/espionagem-ilegal-da-abin-atingiu-30-mil-pessoas-e-dados-foram-guardados-dados-em-israel-diz-chefe-da-pf.ghtml

Taraciuk, T. (2022, febrero 24). En El Salvador, leyes amplias sobre delitos informáticos amenazan derechos fundamentales. Human Rights Watch. https://www.hrw.org/es/news/2022/02/24/en-el-salvador-leyes-amplias-sobre-delitos-informaticos-amenazan-derechos

Tarazona, D. (2024, junio 6). Violencia en Latinoamérica: El 80% de los asesinatos contra defensores de derechos humanos ocurrió en la región. Mongabay. https://es.mongabay.com/2024/06/violencia-latinoamerica-asesinatos-contra-defensores-informe/

The Carter Center. (2024, julio 30). Declaración del Centro Carter Sobre la Elección en Venezuela. The Carter Center. https://www.cartercenter.org/news/pr/2024/venezuela-073024-spanish.pdf

VE sin Filtro. (2023). Reporte sobre la situación de los derechos humanos digitales en Venezuela. VE sin Filtro. https://vesinfiltro.com/res/files/reporte-2022-2023.pdf

@vesinfiltro. (2024, febrero 2). X [Post]. X. https://x.com/vesinfiltro/status/1753542563280093687

X. (2024). [Software]. https://x.com/search?q=”defensores” AND “delincuentes” until%3A2024-01-15 since%3A2024-01-09&src=typed_query&f=live

Xinhua Español. (2024, noviembre 21). Constelación de satélites comerciales de China proporcionará servicios de internet a Brasil. Xinhua Español. https://spanish.news.cn/20241121/bb9137066179416283f657a00b868259/c.html

Yuhas, A. (2023, febrero 17). Seré nicaragüense hasta el día que me muera: El gobierno de Ortega retira la ciudadanía a cientos de personas. The New York Times. https://www.nytimes.com/es/2023/02/17/espanol/nicaragua-quita-ciudadania-disidentes.html

derechosdigitales.org