En la mira: seguridad y principales amenazas digitales en América Latina

DERECHOS DIGITALES
América Latina

EN LA MIRA: SEGURIDAD Y PRINCIPALES AMENAZAS DIGITALES EN AMÉRICA LATINA

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

Supervisión general: Rafael Bonifaz y Mayra Osorio

Autor: Valentín Díaz

Revisión y corrección de Textos: Rafael Bonifaz, Mayra Osorio y Juan Carlos Lara

Traducción al inglés y al portugués: Inglés-Gonzalo Bernabó / Portugués-Dafne Melo

Diseño: 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).

ÍNDICE

EN LA MIRA: SEGURIDAD Y PRINCIPALES AMENAZAS DIGITALES EN AMÉRICA LATINA

REPORTE - DICIEMBRE 2023-MAYO 2024

1.INTRODUCCIÓN

La defensa de los derechos humanos en el espectro digital es una tarea que se ha llenado de obstáculos en América Latina, en medio de un auge de gobiernos que utilizan la tecnología como un arma contra la disidencia política y una creciente presencia de actores criminales en línea. En este panorama, suceden ataques cibernéticos con afectaciones a servicios públicos, recolección masiva y abuso de los datos personales por entidades públicas y privadas, espionaje estatal y hostigamiento dirigidos a diversas comunidades en riesgo como personas defensoras de los derechos humanos y diversidades, activistas y periodistas. Estas son solo algunas de las amenazas y violaciones a los derechos humanos en línea a las que se encuentran expuestos actores de la sociedad civil en la región más peligrosa del mundo para líderes sociales (Tarazona, 2024).

Internet se ha convertido en un espacio esencial para ejercer el activismo y la defensa de los derechos humanos, por lo que mantenerlo libre, abierto y seguro se convierte en un imperativo para garantizar el ejercicio de derechos. Por ello, bajo un contexto hostil a escala regional, la defensa de los derechos humanos en el espacio digital requiere de esfuerzos transfronterizos cada vez mayores. Particularmente en el campo de la seguridad y el análisis de amenazas digitales con enfoque social crítico, el monitoreo y la atención de casos por parte de distintas organizaciones carecen de compilación y sistematización como fenómenos regionales.

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 trabajan en la defensa de los derechos humanos en línea, que han decidido unir esfuerzos para mejorar el entendimiento del comportamiento de los incidentes de seguridad digital desde una perspectiva regional.

OLAD se empezó a conformar en 2021 y pasó por varios procesos de maduración hasta la publicación de este informe. Hoy en día forman parte de esta alianza las organizaciones Código Sur (regional), Colnodo (Colombia), Conexión Segura (Venezuela), Derechos Digitales (regional), Escola de Ativismo (Brasil), Fundación Acceso (regional), Fundación InternetBolivia.org (Bolivia), Fundación Karisma (Colombia), Instituto Nupef (Brasil), LaLibre.net Tecnologías Comunitarias (Ecuador), MariaLab (Brasil), Social TIC (México), Sursiendo (México) y Taller de Comunicación Mujer (Ecuador).

Cada una de las organizaciones del OLAD cumple diferentes funciones en sus respectivos espacios geográficos y dentro de los contextos particulares de cada país. Mientras algunas de ellas se enfocan, por ejemplo, en la investigación y acompañamiento de casos de ciberespionaje o censura a activistas y periodistas, otras dedican sus esfuerzos a la democratización de la tecnología y a la protección de grupos en situación de vulnerabilidad o marginalización histórica frente a los ataques en espacios digitales que son a su vez expresiones de prejuicios basados en múltiples desigualdades de género, raza, clase social, identidad sexual, edad o condición de discapacidad.

En octubre de 2023, varias integrantes del OLAD tuvieron una reunión presencial en Santiago, Chile, donde acordaron llevar a cabo la realización del informe *En la mira*, un seguimiento colaborativo a incidentes de seguridad digital. Este reporte recopila así el trabajo articulado de estas organizaciones, en un período fijado entre diciembre de 2023 y mayo de 2024. De igual manera, pretende contribuir con observaciones a los procesos del Observatorio mediante la identificación de fortalezas y retos a futuro, tomando en cuenta las complejidades típicas del trabajo colaborativo.

2.METODOLOGÍA

El informe *En la mira* está construido bajo una metodología mixta, que fusiona el análisis de datos recopilados en el trabajo diario de las organizaciones con experiencias cualitativas surgidas de discusiones en las distintas fases de trabajo con el Observatorio.

Para ello, se diseñaron dos formas de recopilar la información. La primera es un esfuerzo conjunto de monitoreo del contexto en asuntos de seguridad digital en América Latina, al cual para efectos de comprensión este informe llamará en adelante "monitoreo de contexto". La segunda es una esquematización de una serie de datos recopilados a partir de los casos atendidos por cada organización que forma parte del OLAD, a la cual este informe se referirá como "reporte de casos propios". Para ambos procesos, se delimitó un período de recolección de información que va de diciembre de 2023 a mayo de 2024.

Para el monitoreo de contexto, el equipo de OLAD fue recolectando una serie de entradas de información documental. Se llevó a cabo una curaduría de artículos de prensa y publicaciones de la sociedad civil sobre incidentes y amenazas digitales relevantes registrados en América Latina durante el período señalado y se levantaron reportes mensuales que facilitaron la realización de un análisis general de lo ocurrido en esos seis meses. Entre los incidentes analizados se encuentran ciberataques que han afectado a infraestructura pública y servicios estatales en los países estudiados, situaciones de ciberacoso y censura a activistas, así como graves violaciones a los derechos humanos a través del uso de tecnologías de vigilancia contra la sociedad civil, entre otros hechos relevantes.

Por otro lado, el reporte de casos propios está compuesto por una recolección de datos con base en los casos atendidos por cada una de las organizaciones que participan en OLAD, desde sus propios mecanismos, protocolos de atención y medidas de anonimización de datos. Al ser el Observatorio una unión de organizaciones de diferente naturaleza trabajando en distintos contextos, los datos recopilados para el reporte de casos propios son de igual manera diversos, por lo que no deben verse como una medición comparativa entre casos, países u organizaciones.

Es necesario anotar que el reporte presenta un sesgo de limitación relacionado con las líneas temáticas de cada organización que forma parte del OLAD, por lo cual las cifras y

los números presentados en el reporte de casos propios deberán ser analizados desde miradas diferentes a la tendencia natural de este tipo de informes a generar rankings. Por el contrario, dichos datos deberían ser analizados como una representación del trabajo de atención de casos que realizan las organizaciones pertenecientes al Observatorio.

A pesar de estas dispersiones, el equipo de OLAD pudo identificar cuatro problemáticas comunes que abordan las organizaciones que forman parte del proyecto. Estas son vigilancia y espionaje, violencia de género en espacios digitales, ataques a infraestructura crítica, y vulneraciones a la libertad de expresión en línea en los países donde las organizaciones trabajan.

Los casos documentados por las organizaciones, entre 2023 y 2024, se dividieron en tres periodos. El primer reporte recolectó datos entre diciembre de 2023 y enero de 2024, y recopiló 163 casos; el segundo se llevó a cabo de febrero a marzo de 2024, con 135 casos; y un último de abril a mayo de 2024, que contabilizó 113 casos. En total, fueron 411 casos atendidos por las organizaciones, en un periodo que va de diciembre de 2023 a mayo de 2024.

3. CONTEXTO DE SEGURIDAD DIGITAL EN AMÉRICA LATINA

La presente sección ofrece un vistazo al panorama coyuntural de vulneraciones e incidentes de seguridad digital suscitados en la región durante el período cubierto. Este capítulo, como se indicó en el apartado metodológico, se construyó con base en una selección de artículos de prensa e informes sobre casos de ataques y vulneraciones digitales de amplia magnitud o impacto social y que, a su vez, afectaron a distintos grupos históricamente discriminados. Cabe mencionar que los incidentes detallados en esta sección no corresponden a la totalidad de eventos registrados en la región durante el período asignado, sino que se trata de una muestra que resulta de un trabajo de monitoreo constante.

3.1 BOLIVIA

Durante el período abarcado por este informe, Bolivia vivió uno de los periodos de polarización política más intensos en los últimos años. Una evidente ruptura en el partido oficialista (Molina, 2023) separó a los leales al gobierno de Luis Arce de aquellos que se mantenían en línea con el expresidente Evo Morales. Mientras tanto, en junio de 2024 un fallido intento de golpe de estado (BBC News Mundo, 2024) terminó de crispar la ya dividida opinión pública.

Con un 62% de su población autorreconocida como indígena (Instituto Nacional de Estadística de Bolivia, 2024), el músculo social de la política partidista boliviana se cimienta sobre su población rural. La coyuntura política nacional repercute asimismo en la organización comunitaria, pues el actual partido oficialista se origina en organizaciones de base con enfoque plurinacional (Do Alto, 2007).

En mayo de 2024, LatAm Journalism Review publicó una recopilación de investigaciones de organizaciones locales que estudiaron el fenómeno de la desinformación que se difunde en comunidades rurales en Bolivia, Perú y El Salvador (Knoerr, 2024). Particularmente en Bolivia, según una investigación de ChequeaBolivia, en tres localidades rurales (Villa Tunari, Cochabamba; Yacapaní y Montero, Santa Cruz) la desinformación en línea se intensificó durante la crisis política y electoral de 2019, que terminó con la salida de Evo Morales del poder y masivas protestas, con gran participación de organizaciones rurales, contra el gobierno transitorio de Jeanine Añez que dejaron decenas de muertos (ChequeaBolivia, 2024). El informe evidencia que la población indígena, durante aquellos eventos, estuvo particularmente expuesta a la desinformación. Ya en un nuevo gobierno, pero aún bajo un contexto polarizado, las comunidades rurales podrían ser sometidas a nuevos intentos de manipulación del discurso público.

3.2 BRASIL

En abril de 2024, la justicia brasileña abrió una investigación contra el magnate Elon Musk, accionista mayoritario de X (antes Twitter), y lo señaló como responsable de una "instrumentalización criminal" para obstruir a la justicia (Folha de Sao Paulo, 2024), luego de la reactivación de varias cuentas de usuarios que el poder judicial había ordenado cerrar al considerarlas amplificadoras de desinformación. Musk respondió entonces con una serie de descalificaciones públicas sobre el juez que tomó la decisión (DW, 2024). El hecho ahondó la crisis de relaciones entre la plataforma y el gobierno, que terminó con

la suspensión temporal de la red social a escala nacional por orden un juez del Supremo Tribunal Federal (STF), bajo la exigencia de que la compañía nombrara a un representante legal en Brasil, el segundo mayor mercado para X en el mundo (BBC News Mundo, 2024).

A este panorama se adhiere el hecho de que Elon Musk es también dueño de la compañía de internet satelital Starlink, cuyo volumen de tráfico según el reporte anual de Cloudflare Radar de 2023 se triplicó ese año en Brasil, especialmente en zonas rurales no cubiertas (Belson, 2023). El gobierno buscaba alternativas a esa dependencia y en noviembre de 2024 firmó un memorando con China para utilizar su constelación de satélites comerciales y así ofrecer conexión de banda ancha a zonas remotas (Xinhua Español, 2024).

Los conflictos legales entre el gobierno brasileño y X ocurrieron luego del cambio de propietario de la plataforma tras un complejo proceso de compra hostil por parte de Musk (BBC News Mundo, 2024). En 2022, la plataforma entonces llamada Twitter, accedió a una serie de normas restrictivas ordenadas por el máximo tribunal electoral brasileño (TSE) para resguardar a la elección presidencial del impacto de la desinformación. La normativa dejaba en manos del tribunal la atribución de decidir qué contenido debía ser eliminado de la plataforma, so pena de elevadas multas por cada hora de retraso en los esfuerzos de moderación (Chambers, 2022).

El entonces mandatario Jair Bolsonaro y varios de sus partidarios se habían pronunciado constantemente, desde tiempo atrás, sobre supuestas faltas de transparencia del TSE y, en varias ocasiones, sembraron dudas sobre la confiabilidad del sistema de voto electrónico del país (Díaz, 2022). A pesar de las restricciones impuestas por el TSE a las principales plataformas y del silencio que guardó Bolsonaro tras la difusión de los resultados que dieron por ganador a Lula, en 8 de enero de 2023, miles de seguidores del candidato vencido electoralmente invadieron y vandalizaron los edificios del Congreso, la Presidencia y el Supremo Tribunal Federal (STF) (BBC News Mundo, 2024). Tras la compra de Musk, la Corte Suprema de Justicia abrió una investigación contra el magnate por supuestamente fallar en la contención de desinformación dirigida hacia el TSE (Biller & Sá Pessoa, 2024).

También en abril, una extensa investigación de The Influence Industry Project analizó cómo la desinformación electoral en las plataformas de Meta (Facebook, Whatsapp e Instagram) jugó su rol en los intentos de desestabilización democrática de 2023 (Maia, 2023). En mayo, el poder judicial brasileño firmó un acuerdo de entendimiento con varias empresas, entre ellas Meta, TikTok, Google, Kwai y LinkedIn, para redoblar esfuerzos contra la desinformación (Abrão, 2024).

La corresponsabilidad de las plataformas en torno a la integridad electoral, la defensa de la democracia y la confianza en la institucionalidad democrática del país son asuntos que se han discutido profusamente en Brasil. En esa búsqueda, los diferentes poderes del Estado han adoptado normativas e instalado debates, parlamentarios y también dirigidos hacia la sociedad civil, desde hace varios años (Global Freedom Of Expression Columbia University, 2020). En ese camino, Brasil se ha encontrado no solo con la resistencia frontal de Musk, sino también con el constante lobby que generan un puñado de empresas big tech para ralentizar o torpedear proyectos de regulación (Colombo, 2024). En enero de 2024, por ejemplo, la Policía Federal concluyó luego de una investigación un "abuso de poder económico" por parte de Google y Telegram contra la aprobación de un proyecto de ley contra la desinformación (Falcão, 2024). En un delicado balance entre la salud de la democracia brasileña y la libertad de expresión, la desinformación continúa siendo uno de los principales retos de un Brasil interconectado.

En diciembre de 2023, el gobierno dio un avance importante en materia de privacidad, al lanzar una aplicación que permite a víctimas de robo bloquear remotamente sus dispositivos, una función que facilita los trámites de denuncia y permite que las víctimas aseguren rápidamente información sensible (EFE, 2023).

En materia legislativa, desde finales de 2023, el Senado discute un proyecto de marco regulatorio sobre la inteligencia artificial (Projeto de Lei n° 2338, 2023), una normativa que, tal y como va en curso, organizaciones locales de derechos humanos y tecnologías han visto con buenos ojos (Coalizão Direitos Na Rede, 2024). En 2024, el Consejo de Comunicación Social del Congreso Nacional se reunió para discutir proyectos de ley que buscan que los contenidos periodísticos sean sujetos a remuneración por parte de las plataformas donde estos se comparten (Câmara dos Deputados, 2024).

En enero de 2024, la Policía Federal anunció una investigación contra exfuncionarios de la Agencia Brasileña de Inteligencia (Abin) durante el gobierno de Bolsonaro, a quienes acusan de haber vigilado ilegalmente a unas 30.000 personas, entre ellas, periodistas y magistrados del STF (Sadi, 2024). Los señalamientos involucran al diputado federal Alexandre Ramagem, que fue director de la entidad en el gobierno de Bolsonaro, supuesto responsable de utilizar de manera ilegal un software de origen israelí llamado FirstMile de la empresa Cognyte, que permite interceptar la posición geográfica de un dispositivo móvil a través sus señales GPS, mediante una alteración del protocolo SS7 que manejan las compañías de telecomunicaciones del país, información que por ley es confidencial (BBC News Brasil, 2024).

En marzo de 2024, una investigación de Intercept Brasil destapó el uso de una herramienta que permite la recolección de información de inteligencia de fuentes abiertas (OSINT) en perfiles privados en Facebook, por parte de más de una decena de organismos públicos (Ameno, 2024). Un hallazgo que trajo a colación nuevamente el rol de los gobiernos y los límites en la recolección de datos personales en aras de la seguridad ciudadana.

3.3 COLOMBIA

Colombia inició el año 2024 perdiendo la oportunidad de aprobar un proyecto de legislación sobre tecnología con enfoque de género. El proyecto pasó a debate en enero y se originó en una orden de su Corte Constitucional para que el Estado comenzara a tratar la violencia de género en el espacio digital (Moreno, 2022). Pero durante debates en el parlamento (Castañeda, 2022), la propuesta inicial fue sujeta a cambios que resignificaron por completo el concepto inicial de la ley, la protección de las personas expuestas a la violencia basada en género (Karisma, 2024). En apenas un cambio en el orden de tres palabras, en mayo el Legislativo dejó la puerta abierta a una nueva gama de definiciones de la violencia digital (Moreno, 2024), que incluye menciones a la protección de funcionarios públicos que hacen levantar sospechas de la comunidad defensora de los derechos humanos en entornos digitales[1].

Por otro lado, en febrero, el gobierno de Gustavo Petro buscó un norte hacia la transformación digital mediante la presentación de su Estrategia Nacional Digital a 2026 (Ministerio TIC, 2024). La estrategia concibe a la transformación digital como una política holística que ha dividido en cuatro pilares: conectividad, infraestructura de datos, confianza y seguridad digital y habilidades o fomento del talento digital.

A principios del año 2024, un ciberataque tipo ransomware[2] a los portales de la aseguradora médica Salud Total generó afectaciones de atención en un sistema con 4,8 millones de afiliados (Rodríguez, 2024). La Superintendencia Nacional de Salud tuvo que pronunciarse, en un país donde el sistema de salud público es administrado por proveedores privados.

1 Tanto la primera versión del proyecto, propuesta en la Comisión Primera Constitucional Permanente del Senado, como las versiones posteriores con las modificaciones mencionadas en este informe aparecen en la gaceta oficial del Congreso de Colombia. En su primera versión, aparece en la gaceta N 605 de 2023. La versión más reciente, que terminó siendo archivada, aparece en la gaceta N 342 de 2024. Ambas se pueden ubicar en el buscador de la gaceta del Congreso (Congreso de la República de Colombia, s/f).

2 Ransomware: Malware que bloquea un dispositivo mediante el cifrado o encriptación de su contenido. Tiene fines extorsivos, pues se pide un rescate por liberar la información (ESET, s/f).

En marzo de 2024, el periodista israelí Gur Meggido, del diario Haaretz, aseguró en una investigación que Colombia pagó 13 millones de dólares en efectivo por la adquisición del software espía Pegasus, del israelí NSO Group (Megiddo, 2024). Meses después, esta misma información fue denunciada por el presidente Gustavo Petro (Beltrán, 2024), que responsabilizó a su antecesor Iván Duque por la compra en 2021, cuando Colombia registraba masivas protestas que duraron varios meses.

En abril, el ministro de Defensa Iván Velásquez reconoció (Revista Semana, 2024), tras la publicación de una investigación periodística (AFP, 2024), la presencia en TikTok de perfiles asociados a la mayor agrupación de frentes disidentes de la extinta guerrilla de las FARC, el Estado Mayor Central (EMC). En la red social de origen chino, los guerrilleros envían mensajes de reclutamiento dirigidos a la juventud colombiana. El general Helder Giraldo, entonces comandante general de las Fuerzas Militares, aseguró que las actividades de las disidencias en esa red social suponen “una flagrante violación al mismo cese al fuego” que en ese entonces regía por la realización de ciclos de conversaciones de paz con el gobierno colombiano.

3.4 ECUADOR

El último tiempo, la crisis de seguridad en Ecuador escaló a nuevos niveles y dejó una tasa de homicidios récord, de 47 por cada 100.000 habitantes en 2023 (Observatorio Ecuatoriano de Crimen Organizado, 2024), la más alta de América Latina. Entre los eventos violentos de mayor relevancia destacan el asesinato del candidato presidencial Fernando Villavicencio en agosto de 2023 (BBC Mundo, 2023) y la ola nacional de violencia armada que el país vivió en enero de 2024 (Cañizares et al., 2024), que trascendió globalmente por la toma de rehenes por parte de un grupo armado a trabajadores de la estación estatal de televisión TC durante una transmisión.

Estos últimos hechos llevaron al presidente Daniel Noboa a decretar el estado de conflicto armado interno, que permitió la militarización del país (BBC News Mundo, 2024). Esta situación originó una serie de violaciones a los derechos humanos, cometidas principalmente por militares, entre casos de ejecuciones extrajudiciales, desapariciones forzadas y cientos de denuncias de tortura en las calles y cárceles del país (Human Rights Watch, 2024). Paralelamente, el gobierno emprendía una campaña de desprestigio contra defensores de derechos humanos que quedaron expuestos ante la narrativa oficial (Amnistía Internacional, 2024), una apología a los abusos militares que también fue profusamente esparcida por usuarios en redes sociales durante los primeros meses de la declaratoria de conflicto (Curipoma, 2024).

En ese contexto el Comité Permanente por la Defensa de los Derechos Humanos (CDH Guayaquil), que representa, entre decenas de víctimas de violaciones a los derechos humanos en Guayaquil, a familias de personas privadas de la libertad, denunció en febrero un ataque cibernético que inhabilitó sus correos electrónicos, lo que la organización calificó como "un acto deliberado de intimidación, resultado de las denuncias del abuso ejercido por las Fuerzas Armadas" (@cdh.gye, 2024). El mismo mes, la ONG de protección de periodistas Fundamedios envió una alerta sobre una serie de ciberataques, más de 300 desde diciembre de 2023, contra el portal periodístico Indómita Media, que publica permanentemente sobre el deterioro de la situación de derechos humanos en Ecuador (Fundamedios, 2024).

Como antesala de estos hechos, en diciembre de 2023 un caso judicial ligado a un narcotraficante fallecido remeció las investigaciones del asesinato del candidato a presidente Fernando Villavicencio (Fiscalía General del Estado Ecuador, 2024). En conversaciones extraídas del teléfono de Leandro Norero, jefe criminal asesinado en una masacre carcelaria en 2022 (BBC News Mundo, 2024), se evidenciaron vínculos entre el narcotraficante y trabajadores del ECU-911, el centro estatal de atención y coordinación de emergencias que maneja una extensa red nacional de cámaras de vigilancia (ECU-911, s/f-a).

Para el bautizado caso Metástasis, la Fiscalía General del Estado liberó una serie de registros de conversaciones de la aplicación Threema de Norero con varias figuras públicas, entre ellos periodistas, policías, guías penitenciarios y funcionarios judiciales. Uno de los chats liberados mostró que Norero habría empleado un software del sistema nacional de atención de emergencias, el ECU-911, para hacer seguimientos a Villavicencio (Bonifaz, 2024), una información que posteriormente fue reconocida por el director de la entidad como un caso de "mal uso" de sus tecnologías en enero de este año (Primicias, 2024). El programa utilizado fue Mobile Locator, un software de geolocalización que, según el mismo ECU-911, ofrece un "posicionamiento aproximado de la llamada realizada por una persona a la línea única de emergencias 911 desde un teléfono" (ECU-911, s/f-b).

En paralelo, la Asamblea Nacional de ese país intentó tramitar una ley de seguridad digital que instalara por primera vez un debate que aborde la prevención y el tratamiento de amenazas digitales y ciberataques. Sin estar exenta de articulados polémicos (Carrillo, 2024), el proyecto pionero significó por lo menos una aceleración del debate público en materia de ciberseguridad. Sin embargo, el proyecto terminó archivado por falta de apoyo político (Asamblea Nacional del Ecuador, 2024).

En diciembre de 2023, la Contraloría General del Estado inició una auditoría al proceso de contratación para la instalación de un sistema de voto por internet ideado para la comunidad migrante de ecuatorianos en el exterior para la primera vuelta de elecciones en agosto de ese año (El Universo, 2023). La implementación de esa tecnología fue un fracaso (La Barra Espaciadora, 2024), ya que la plataforma colapsó y usuarios registraron problemas desde tempranas horas para ejercer su derecho al voto. Más tarde, la presidenta del organismo, Diana Atamaint, aseguró que la plataforma había sido objeto de un ciberataque, por lo que se decidió suspender el conteo de votos e ignorar los resultados para esa población. Posteriormente se conoció que la empresa contratada no tenía ninguna experiencia en la rama.

Por otra parte, en el ámbito judicial, el emblemático caso del informático sueco Ola Bini, acusado por la fiscalía de Ecuador por cargos que han sido ampliamente cuestionados por organizaciones de la sociedad civil (Bonifaz & Silva, 2024), llegó a su fin este año aunque no con el resultado que esperaban su defensa y los organismos defensores de derechos humanos. En un extraño giro y con una argumentación carente de precisión técnica, un tribunal de apelación revirtió una sentencia de primera instancia que lo declaró inocente por el delito de acceso no consentido a un sistema informático (CNN Español, 2024b). Con esa condena, el informático se enfrentaba a un año de prisión, pero días después el mismo tribunal aceptó un pedido de suspensión condicional de la pena. En otras palabras, Ola Bini es un hombre libre, aunque condenado por la justicia. El sueco fue detenido en circunstancias cuestionadas (Electronic Frontier Foundation, 2021), pues su arresto coincidió con la expulsión del fundador de Wikileaks, Julian Assange, de la embajada de Ecuador en Reino Unido, donde el australiano se encontraba asilado desde 2012. Ola Bini y Julian Assange eran amigos cercanos y el entonces presidente Lenín Moreno, de la mano de su ministra del Interior María Paula Romo, vincularon al sueco con supuestos intentos de desestabilización.

3.5 EL SALVADOR

El Salvador, por su lado, vive un proceso reportado de erosión de su democracia bajo el gobierno de Nayib Bukele (Bernal, 2024), que se reeligió este 2024 con la venia del Tribunal Supremo Electoral pese a una prohibición constitucional expresa (CNN Español, 2024). Al igual que en los casos de Venezuela y Nicaragua, que se mencionan más adelante, estos procesos sociales tienen repercusiones en el espectro digital.

Ya en 2022, Human Rights Watch advertía (Taraciuk, 2022) sobre la aprobación de una batería de reformas legales por parte de la Asamblea Legislativa que incluían

modificaciones al Código Penal y la Ley de Delitos Informáticos (Derechos Digitales, 2022), que hacen pasar bajo la categoría de ciberdelitos a conductas, entre otras, como la obtención de material confidencial, algo que pone en riesgo el ejercicio periodístico.

El país ocupó en 2023 el puesto 115 de 180 en el índex de libertad de prensa de Reporteros Sin Fronteras (RSF) y en 2024 bajó 18 puestos y se ubicó en el 133 (RSF, 2024). Como antecedente, en 2022, el Citizen Lab de la Universidad de Toronto publicó una extensa investigación en la que revelan vulneraciones ilegales con el spyware Pegasus a teléfonos de personeros de organizaciones de la sociedad civil y periodistas, entre estas personas, 22 periodistas del portal de investigación El Faro (Gavarrete et al., 2022).

A finales de ese año, un grupo de trabajadores del medio interpuso una demanda ante un tribunal estadounidense contra la firma. Pero en marzo de 2024, la demanda fue desestimada por un juez de California. En su apelación, el grupo de periodistas consiguió el apoyo de los gigantes Microsoft y Google, dos fabricantes cuyos productos fueron vulnerados por Pegasus para acceder a las comunicaciones del personal de El Faro (Gressier, 2024).

3.6 MÉXICO

Desde los últimos dos años, México ha intentado aprobar legislaciones relativas a los derechos humanos en el ámbito digital, la ciberseguridad y el acoso digital, sin mucho éxito en la promoción y discusión de estas ideas, tanto así que tres proyectos federales propuestos por los legisladores se han estancado sin avances (Reyes, 2024).

En enero de 2023, una base de datos personales sensibles de varios reporteros circuló en un foro de filtraciones (Osorio, 2024). Más adelante se supo que la base de datos venía del sistema de acreditación de prensa de la Presidencia para ingresar a las conferencias matutinas del expresidente Andrés Manuel López Obrador. Esto ocurrió en un contexto delicado para el ejercicio del periodismo, pues México es el país sin guerra más peligroso para el ejercicio periodístico (RSF, 2024).

En febrero, el país acaparó titulares con una nueva situación de vigilancia excesiva cuando una investigación de R3D reveló algunas de las actividades del Centro de Operaciones del Ciberespacio (COC) (R3D, 2024a), adscrito a la Secretaría de Defensa Nacional, que bajo la fachada de “operaciones militares en el ciberespacio” monitoreó la actividad de usuarios críticos con el ejército en redes sociales en un intento por influenciar la opinión pública, incluso mediante la utilización de cuentas bot.

Ese mismo mes, el Estado se enfrentó a nuevos escrutinios por el caso Pegasus (Artículo 19, 2024), cuando la Suprema Corte de Justicia ordenó a la Secretaría de Hacienda hacer pública la información recopilada para una investigación hecha por este ente ante la compra y el uso del software espía israelí objeto de centenares de denuncias sobre gobiernos que han utilizado la herramienta para perseguir a activistas, periodistas y disidentes políticos. Con muy lentos avances, el caso Pegasus en México está lejos de cerrarse.

Un mes antes, el único procesado por la intervención ilegal con Pegasus al teléfono de la periodista Carmen Aristegui, el operador Juan Carlos García, había sido absuelto por un juez federal quien consideró que la Fiscalía General de la República no logró probar su participación en el delito (Proceso, 2024). El juez, sin embargo, reconoció que la periodista fue intervenida ilegalmente y consideró que el caso debe seguir siendo investigado pues la fiscalía no ha hecho los esfuerzos suficientes para traer justicia.

Por otro lado, en abril de 2024, el gigante del retail y el crédito de consumo, Coppel, fue ampliamente cuestionado por organismos de la sociedad civil en abril por guardar silencio ante un ciberataque que afectó masivamente sus servicios y cuyas características técnicas nunca fueron aclaradas a los consumidores (R3D, 2024). Voces independientes aseguraron que debía tratarse de un ataque tipo ransomware.

3.7 NICARAGUA

El saldo de medición de los derechos humanos en entornos digitales en Nicaragua es negativo, como señaló ya un informe emitido en septiembre de 2023 (Derechos Digitales, 2023). El documento señala importantes antecedentes que se remontan a las masivas y prolongadas protestas de 2018 que fueron brutalmente reprimidas por el gobierno de Daniel Ortega (OEA, 2018).

Un informe de ese año de la Comisión Interamericana de Derechos Humanos (CIDH) menciona graves violaciones a los derechos humanos que incluyen ejecuciones extrajudiciales, casos de tortura y cientos de detenciones arbitrarias, así como actos de censura contra ciudadanos, periodistas y medios de comunicación (Comisión Interamericana de Derechos Humanos, 2018).

Paralelamente, la represión también se hizo presente en el espacio digital y acciones como la interrupción al acceso a internet, la criminalización de la expresión en línea, los intentos por manipular la opinión pública y la vigilancia masiva de las

telecomunicaciones son solo algunos de los varios desafíos presentados ante la sociedad civil nicaragüense, que debe sortear obstáculos cada vez más complejos.

En febrero de 2023, el gobierno de Ortega implementó la inédita decisión de quitar la nacionalidad nicaragüense a más de 300 personas críticas de su mandato, un hecho transversalmente repudiado por organizaciones de defensa de los derechos humanos (Yuhas, 2023). En enero del año 2024, recién se instaló un marco legal para aquella figura, cuando la Asamblea Nacional de ese país aprobó una reforma constitucional que permite el retiro de la nacionalidad a los ciudadanos condenados por el delito de traición a la patria (EFE, 2024). En septiembre, Ortega volvió a usar este recurso después de excarcelar a más de un centenar de opositores y expulsarlos hacia la frontera con Guatemala (EFE, 2024).

3.8 VENEZUELA

En un año electoral para Venezuela, el primer semestre de 2024 se avizoraba como un preámbulo de lo que finalmente ocurrió en julio y agosto (Consejo de Derechos Humanos de las Naciones Unidas, 2024). El diagnóstico sobre Venezuela para este informe se encuentra limitado sus propios factores metodológicos que establecen una ventana temporal (diciembre de 2023 a mayo de 2024) que impide ahondar en los hechos posteriores a la ampliamente cuestionada reelección de Nicolás Maduro (The Carter Center, 2024) y su posterior proceso de represión política como respuesta a la protesta social. Así, el reporte de contexto para Venezuela en este informe puede considerarse como un análisis sobre políticas y decisiones que aplanaron el camino de cara a la elección.

Ya el Reporte sobre la situación de los derechos humanos digitales en Venezuela 2022+2023, de VE sin Filtro, advertía de la existencia de un aparataje estatal “masivo” para interceptación de telecomunicaciones y de prácticas arbitrarias de las autoridades como la exigencia de acceso a datos y conversaciones personales mediante la confiscación de dispositivos (VE sin Filtro, 2023). El reporte menciona una utilización abusiva del monitoreo en redes sociales, comúnmente dirigido a periodistas y activistas, y la utilización de las mismas para llevar a cabo intimidaciones, amenazas y difundir discursos estigmatizantes contra la disidencia política. También ahonda en el problema de la escasa y precaria conectividad que tiene un venezolano promedio, que además se ve constantemente diezmada por los recurrentes cortes de energía a lo largo del país.

El informe anual de derechos digitales de 2023 Algoritmos del Silencio arrojó una cifra de 128 violaciones a los derechos humanos en el ciberespacio dirigidas a periodistas,

ciudadanos y organizaciones de la sociedad civil (Instituto Prensa y Sociedad, 2023). El documento también señala que, durante ese año, 46 medios de comunicación independientes permanecían bloqueados por proveedores de internet que operan en el país. Algunos de esos nuevos bloqueos se reportaron unos meses antes de las elecciones, como en los casos de los portales El Político, Impacto y La Gran Aldea (Espacio Público, 2024).

En febrero de 2024, Digitel, una de las empresas de telefonía más grandes del país, sufrió un ataque ransomware que puso en riesgo los datos personales de miles de usuarios y evidenció la débil infraestructura con la que trabajan varias de las principales empresas del país (@vesinfiltro, 2024).

En abril, el oficialismo promovió un proyecto llamado Ley contra el fascismo, neofascismo y expresiones similares, que incluye una definición muy abierta sobre conductas que considera "fascistas" y expone a las personas a penas de cárcel por ellas, que de acuerdo con organizaciones no gubernamentales, podría surtir un efecto limitador de la libertad de expresión en el país (Programa Venezolano de Educación Acción en Derechos Humanos, 2024).

En mayo, el actual ministro de Relaciones Exteriores de Venezuela, Diosdado Cabello, anunció en su programa de televisión la introducción de un proyecto de ley que busca limitar la llegada de fondos del extranjero para organizaciones de la sociedad civil (Con el Mazo Dando, 2024). La posibilidad de incluir en el ordenamiento jurídico venezolano una legislación de este tipo ya había sido barajada en 2022 y 2023 (Calderón, 2024). Finalmente, días después de la reelección de Maduro, la ley fue aprobada por mayoría en la Asamblea Nacional (Amnistía Internacional, 2024).

4. ÁREAS TEMÁTICAS Y CASOS DE ESTUDIO

Esta sección contiene una categorización de una serie de sistematizaciones de información de distintas fuentes. Algunas de estas esquematizaciones están basadas en datos y otras tienen que ver con experiencias comunes que han sido discutidas y patrones que han sido identificados de manera orgánica durante los distintos encuentros organizados por el Observatorio.

El capítulo pretende profundizar y puntualizar en cada uno de los cuatro ejes temáticos que el Observatorio pudo identificar en su articulación con las diferentes organizaciones: violencia de género en espacios digitales, ataques a infraestructura, vigilancia y espionaje y vulneraciones a la libertad de expresión en línea.

Como se mencionó anteriormente, los datos recopilados para la elaboración de este informe fueron recogidos en tres etapas temporales: un primer período de diciembre de 2023 a enero de 2024 que recopiló 163 casos; otro de febrero a marzo de 2024, con 135; y un último de abril a mayo de 2024, con 113.

4.1 VIOLENCIA DE GÉNERO DIGITAL

Diferentes formas de expresión en línea de violencia basada en género han resultado un eje casi transversal en el trabajo de la mayoría de organizaciones que hacen parte de OLAD. Por esa razón, y debido a la cantidad de casos atendidos, el Observatorio pudo llevar a cabo una recopilación de datos que permite un ejercicio de mayor profundización.

Las organizaciones que forman parte del OLAD y que atendieron casos de violencia basada en género en el espacio digital durante los respectivos periodos para este informe fueron Derechos Digitales (regional), Fundación Acceso (regional), Fundación Internet Bolivia (Bolivia), La Libre (Ecuador), MariaLab (Brasil), SocialTIC (México) y Taller de Comunicación Mujer (Ecuador).

Tres de estas organizaciones manejan líneas de ayuda directa y ofrecen acompañamiento y respuesta en casos de violencia de género digital. Las iniciativas atienden a mujeres, infancias, activistas, colectivos en defensa de los derechos humanos y personas que forman parte de la comunidad LGTBQA+. Estos proyectos son: el Centro S.O.S Digital de Fundación InternetBolivia.org (Bolivia), Maria d'Ajuda de Marialab (Brasil) y Navegando Libres de la Red de Taller Comunicación Mujer (Ecuador). Sobre este particular, está disponible también el informe *Líneas de ayuda para atender casos de violencia de género en entornos digitales: Monitoreo y tendencias en Bolivia, Brasil y Ecuador* que ahonda sobre patrones comunes con respecto a violencia de género digital en la región (Araújo et al., 2024).

Durante el primer período temporal establecido por el Observatorio –de diciembre de 2023 a enero de 2024– las organizaciones reportaron un total de 28 casos atendidos. En el segundo período –de febrero a marzo de 2024–, el número de casos analizados

ascendió de manera considerable hasta los 50, una cifra que representa casi un tercio de todos los casos reportados en las diferentes líneas de trabajo. Finalmente, durante el tercer período –de abril a mayo de 2024– se contabilizaron 40 casos.

Dentro de este flujo de trabajo se pudo identificar algunos patrones comunes en la naturaleza de los casos abordados principalmente por organizaciones que luchan contra la violencia basada en género, por lo que fueron divididos en grupos temáticos que han sido planteados de una forma amplia, debido a que la caracterización de cada fenómeno puede variar de acuerdo a los criterios de cada organización. El primero corresponde a casos de acoso digital[3], que durante los tres periodos temporales estudiados sumó 39 incidentes. El segundo grupo se engloba en la problemática de la difusión de contenido íntimo o sexual sin el consentimiento de la persona involucrada[4]. En los tres periodos estudiados, esta categorización alcanzó un total de 33 casos. El tercer grupo está conformado por registros de vulneraciones a cuentas de plataformas sociales que pertenecen a mujeres o a agrupaciones de mujeres dedicadas al activismo en sus diferentes facetas. Dentro de estas facetas, aunque no de manera exclusiva, está muy presente el activismo feminista. La sumatoria de casos en este grupo, durante los tres periodos analizados, es de 24.

En todas estas expresiones de violencia de género en línea, los datos reportados por las organizaciones muestran que, en su gran mayoría, este tipo de ataques van dirigidos a personas particulares y que también, en la mayoría de casos, los agresores suelen ser personas particulares. Sin embargo, es visible también un porcentaje considerable de casos en los que el agresor no pudo ser identificado.

3 En el informe *Líneas de ayuda para atender casos de violencia de género en entornos digitales: Monitoreo y tendencias en Bolivia, Brasil y Ecuador*, en el cual se utilizó otra ventana temporal de estudio, dos de las organizaciones que forman parte de OLAD (InternetBolivia.org y la Red de Taller Comunicación Mujer) reportaron que el acoso digital fue la segunda violencia digital más comúnmente reportada por sus líneas de ayuda.

4 Este tipo de casos se engloban en la caracterización de violencia sexual digital que hace la línea de ayuda Navegando Libres por la Red de Taller Comunicación Mujer, que en el informe *Líneas de ayuda para atender casos de violencia de género en entornos digitales: Monitoreo y tendencias en Bolivia, Brasil y Ecuador* se identifica como el tipo de violencia digital más atendido por la organización. En el caso de Maria d'Ajuda de Marialab, este comportamiento se caracteriza como exposición de imágenes íntimas y es el tercer tipo de violencia más atendido por dicha línea. Por otro lado, el Centro S.O.S Digital de Fundación InternetBolivia.org, en el mismo informe, engloba a esta problemática dentro de la categoría de abuso sexual a través de Tecnologías de la Información (TIC), que incluye varias formas de violencia como amenazas y extorsiones a las víctimas relacionadas con la potencial publicación de contenido íntimo.

4.2 ATAQUES DE INFRAESTRUCTURA

Otro de los ejes de interés para el Observatorio son las vulneraciones a sitios web e infraestructura crítica para organizaciones en defensa de los derechos humanos, en su más amplio espectro. En los periodos establecidos para la creación del informe, más de medio centenar de casos fueron atendidos por las organizaciones que componen el OLAD.

La gran mayoría de casos tomados en cuenta para este informe fueron reportados por La Libre, una pequeña organización basada en Ecuador que busca proveer de infraestructura tecnológica "sólida y accesible" a organizaciones, personas y movimientos sociales que trabajan en defensa de los derechos humanos, la naturaleza, la justicia y la igualdad. Entre diciembre de 2023 y mayo de 2024, La Libre atendió al menos 34 casos relacionados con ataques a sitios web de organizaciones sociales y activistas. También atendió 22 casos de ransomware o secuestro de datos.

La disparidad en los datos reportados en esta sección se debe principalmente a que parte fundamental del trabajo de La Libre es, justamente, ayudar con la construcción y el mantenimiento de la infraestructura, así como ofrecer apoyo técnico a las organizaciones.

La Libre está presente en varios países aunque principalmente trabaja en Ecuador. Su cofundador, Jonathan Finlay, asegura para el reporte *En la mira* que la organización trabaja desde hace 10 años "desarrollando infraestructuras autónomas, implementando servicios, proveyendo soluciones de tecnología orientadas a defensores, defensoras de derechos humanos y de la naturaleza".

El enfoque de La Libre está "orientado al acompañamiento", al tejer redes con otras organizaciones sociales "para ir fortaleciendo las luchas". "En algunos casos (las organizaciones) nos buscan porque están sufriendo o han sufrido un ataque, porque han perdido y quieren recuperar información, o aplicaciones, sitios web, redes. O, simplemente, su organización requiere mejorar la infraestructura física de sus telecomunicaciones, o un rediseño del sitio web", asegura Finlay.

Es decir, La Libre ofrece una amplia gama de servicios digitales ideados especialmente para las necesidades de organizaciones y personas defensoras de derechos. La diferencia principal con servicios comerciales comunes es que "la gente que trabaja derechos humanos suele estar en condiciones que no son las mismas a las de una empresa o de un banco", explica. Por eso, las organizaciones "quieren trabajar con

alguien que entienda lo que están haciendo". La idea es dar un "soporte cercano", algo que no necesariamente tiene que ver con aspectos técnicos.

No todo abordaje de las amenazas digitales se remite solo a la parte técnica. En casos de ransomware, por ejemplo, cuando la encriptación de un sistema fue completada, la atención se centra más en "acompañamiento y recomendaciones, primero para que no vuelva a suceder, y segundo para que puedan recuperar la mayor cantidad de información que fuera posible en el menor tiempo".

A finales de 2023, "hubo un momento que sucedió en varias organizaciones que, por distintos medios y con distintos programas de malware, terminaron siendo infectados dispositivos" en ataques de ransomware casi simultáneos. Principalmente fueron afectadas laptops y computadoras de escritorio, pero la organización también registró dos casos de infección a servidores. Finlay señala que los ataques se dieron en el marco de "campañas de grupos de amenazas" que enviaron correos electrónicos tipo phishing[5] dirigidos a las áreas administrativas de las organizaciones y que terminaron infectando los equipos.

Otro tipo de casos, como los ataques a sitios web, pueden ser abordados de manera reactiva. Estos suelen ser "ataques de denegación de servicio[6], adivinación de contraseñas mediante fuerza bruta, infección con malware de sitios web" o casos en los que se han utilizado técnicas de phishing "para hacerse de las credenciales del sitio web y tomar control temporal".

Cuando este tipo de casos llegan, La Libre hace una evaluación del caso "dependiendo de cada escenario". Según la naturaleza del ataque, las soluciones técnicas pueden resultar sencillas o, en casos más complejos, la recuperación del control sobre un sitio web o red puede llegar a ser un proceso largo y engorroso.

5 Phishing: Técnica maliciosa de ingeniería social que consiste en el envío de correos electrónicos, mensajes de texto, llamadas o sitios web fraudulentos para engañar al usuario e inducirlo a compartir sus datos personales, sus credenciales de acceso a alguna plataforma u obligarlo a descargar algún tipo de malware en su dispositivo (Kosinski, 2024).

6 Ataque de denegación de servicio: Un tipo de ciberataque malicioso que consta de una interrupción de un servicio. Suele funcionar mediante la sobrecarga de solicitudes en un sitio web, por ejemplo, lo que causa una interrupción del servicio cuando el servidor recibe más solicitudes de las que puede procesar al mismo tiempo (Cloudfare, s/f).

4.3 VIGILANCIA Y ESPIONAJE

Los casos de México y El Salvador, descritos en el capítulo de contexto regional, dan cuenta de la gravedad de aquellos casos en que el uso de tecnologías de espionaje, supuestamente fabricadas para ejercer el dominio de la ley, fueron utilizadas para objetivos políticos o personales de quienes tienen la capacidad de utilizar el monopolio de la fuerza del Estado.

El caso de El Salvador con Pegasus es algo más reciente que el de México, donde los primeros reportes del uso de Pegasus datan de 2017 (BBC Mundo, 2017). Sin embargo, la magnitud de su uso no fue revelada sino hasta la publicación de un proyecto periodístico transnacional en 2021 que reveló una serie de interceptaciones a cientos de personalidades entre periodistas, activistas y funcionarios gubernamentales alrededor del mundo (Forbidden Stories, 2021).

Solo en México, el gobierno de Enrique Peña Nieto usó el spyware[7] contra 15.000 personas, entre ellos, familiares de las víctimas de la masacre de Ayotzinapa en 2014 (Romero, 2021). En ese país, una organización miembro de OLAD trabaja desde años con asuntos de espionaje estatal: SocialTIC. En abril de 2023, la organización publicó un informe en conjunto con el Centro Prodh, R3D y Article-19 que reveló evidencia de nuevos casos de espionaje con Pegasus por parte del ejército contra defensores de derechos humanos del Centro Prodh (Centro PRODH et al., 2023). Apenas un mes después, el New York Times revelaba otro gran caso según el cual el subsecretario de derechos humanos, Alejandro Encinas, fue interceptado (Kitroeff & Bergman, 2024).

En México, las organizaciones siguen un flujo de trabajo coordinado para atender casos de vigilancia ilegal con Pegasus. Mediante una alianza llamada Coalición de Derechos Digitales conformada por SocialTIC, R3D, el Centro Prodh y Artículo 19. Así, “cada organización tiene un rol muy conciso” cuando llega un caso, asegura Paúl Aguilar, coordinador de seguridad digital de SocialTIC.

R3D se encarga de la representación legal de la víctima, Article-19 documenta las vulneraciones a la libertad de expresión y el Centro Prodh las violaciones a los derechos humanos que se pueden presentar en cada caso. SocialTIC, por su lado, se encarga de la parte técnica: analizar los dispositivos y otras acciones. Esta tarea en muchas ocasiones se hace en colaboración con el CitizenLab de la Universidad de Toronto.

7 Spyware: Software diseñado para recopilar datos confidenciales de un dispositivo sin el consentimiento de su dueño. Por lo general, el spyware se instala en un dispositivo mediante engaños (Kaspersky, s/f).

Pero el trabajo de SocialTIC no se limita solo a la detección del spyware. La organización también implementa una serie de capacitaciones con las víctimas "para ayudarles a configurar sus dispositivos" y tomar las medidas necesarias para una situación similar "no se pueda repetir" o, por lo menos, "hacerlo más difícil para el atacante".

SocialTIC brinda "atención permanente a personas que pudieran o han sido vigiladas" por cualquier tipo de medio. Lo hacen de manera individual y "sobre todo con periodistas que han sido espiados" anteriormente y de quienes existen nuevas sospechas de intervención. "Eso habla de que se está viendo una reincidencia en los casos", sostiene Aguilar. En algunos casos, se trata de Pegasus, pero otros "tienen que ver con indicios de otras tecnologías que al parecer se están usando" en México. Pero no solo se trata de spyware, sino también de interceptación de comunicaciones, monitoreo invasivo en redes sociales, seguimiento físico e incluso campañas de acoso en redes. "Es una acción de vigilancia y espionaje mucho más amplia, no solamente enfocada a spyware", dice Aguilar.

Por otra parte, SocialTIC lleva a cabo trabajo con organizaciones que acompañan a grupos de personas que han sido vigiladas. Estos acompañamientos son "mucho más amplios ya que implican poder trabajar con la organización completa", asegura. México se organiza políticamente bajo un sistema federal descentralizado, que otorga a los estados que lo componen una serie de atribuciones que incluyen sistemas de seguridad propios, a nivel municipal y estatal. Y si bien Pegasus se vende solo a gobiernos centrales y sus organismos de defensa, la utilización de otras tecnologías de vigilancia y espionaje en los estados se encuentra en auge.

"Hay otras tecnologías que los estados están comprando, tal vez de menor gama. Entonces, pareciera que están teniendo acceso a otros tipos de spyware, menos sofisticados, a otras tecnologías también de intervención de comunicaciones y rastreo, menos sofisticadas. Va en proporción a sus capacidades económicas", señala Aguilar y agrega que "hay evidencia de que casi los 32 estados han comprado tecnologías de este tipo (...) Estamos trabajando en demostrar en que las han usado contra sociedad civil".

4.4 VULNERACIONES A LA LIBERTAD DE EXPRESIÓN EN LÍNEA

El último gran eje de observación del OLAD son las vulneraciones a la libertad de expresión en línea. En esa área, las organizaciones que forman parte del Observatorio atendieron un total de 92 casos de ataques a la libertad de expresión en sus respectivos países.

En esta categoría reportaron atención de casos Derechos Digitales, Marialab, SocialTIC, La Libre, Fundación Internet Bolivia y Sursiendo. Entre todas las organizaciones se llevó a cabo la recuperación de 34 cuentas de redes sociales. De diciembre de 2023 a enero de 2024 fueron 19; de febrero a marzo de 2024, 9; y de abril a mayo de 2024, 6. Las recuperaciones de cuentas –que pueden ser arrebatadas debido a ciberataques o esfuerzos masivos de denuncia– se llevaron a cabo ante Facebook, Instagram, X (antes Twitter) y Whatsapp. A modo de caracterización general, los perfiles cuyos casos se atienden con prioridad suelen ser de personas vinculadas a la defensa de derechos, el activismo social y ambiental y la búsqueda de justicia e igualdad.

Otro ángulo de este fenómeno se puede observar a través del registro de campañas de desprestigio y difamación, en ocasiones, coordinadas. De diciembre de 2023 a enero de 2024, las organizaciones reportaron 20 casos bajo esta categoría; entre febrero y marzo de 2024, 14; y de abril a mayo de 2024 han sido 24.

En esa subcategoría, nuevamente destacan los números de La Libre, pues en los tres periodos temporales, la sumatoria de casos atendidos por todas las organizaciones es de 58. De ese total, 51 fueron atendidos por La Libre, en Ecuador.

En el capítulo sobre contexto regional, se mencionó la coyuntura hostil que existe contra defensores de derechos humanos en Ecuador a partir de la declaratoria de conflicto armado interno en enero de 2024. Es vital tomar en cuenta este contexto de estigmatización a las personas defensoras de derechos humanos al mencionar los casos atendidos por La Libre. Cuando se trata de campañas de desprestigio, La Libre trabaja principalmente con asesoría a las personas afectadas.

A inicios de año, cuando el presidente de Ecuador decretó la guerra interna, “había campañas que parecían organizadas por grandes equipos de personas muy afines al gobierno que buscaban afectar a organizaciones que pedían respeto de derechos humanos”. Varias organizaciones de defensa de derechos humanos, como el Comité Permanente por la Defensa de los Derechos Humanos, que ofrece asesoría gratuita a víctimas de crímenes de estado, fueron señaladas por cientos de cuentas de manera simultánea.

Una búsqueda en X, antes Twitter (X, 2024), filtrada entre el 9 y el 15 de enero, con las palabras claves “defensores” y “delincuentes”, arroja cientos de resultados como este: “Excelente trabajo @ffaa (cuenta de las Fuerzas Armadas), y a estos sopas defensores de delincuentes hay que darles cariño igual”, dice un usuario comentando un video ciudadano donde se ven actos de tortura por parte de militares. La palabra clave “Rulay”

también lleva a dicha tendencia. Es el nombre de una canción atribuida a un grupo criminal que terminó convertida en la banda sonora, a modo de meme, de decenas de videos de militares ejerciendo torturas.

Durante las primeras semanas de declaratoria de conflicto armado, "era evidente que había agencias del estado que volcaron sus esfuerzos, sobre todo de equipos de comunicación y consultores, que se enfocaron en realizar estos ataques", sostiene. "Era súper violento. Y era constante y permanente", denuncia.

Finlay recuerda el caso de una organización que trabaja con personas privadas de la libertad que fue objeto, primero, de comentarios estigmatizantes y violentos en redes sociales. Poco después, los comentarios pasaron a ser amenazas, por correo electrónico y llamadas insistentes.

"En ese caso particular, lo que se hizo fue un proceso de acompañamiento en el que se plantearon estrategias de cómo bloquear, por salud mental, esta interacción". En este panorama, se implementaron acciones como asesorías sobre configuraciones para bloquear y aislar el contenido en redes sociales, diseño de protocolos en caso de amenazas, capacitaciones sobre bloqueo de llamadas, etc. Todo esto Finlay lo define como "un acompañamiento en seguridad digital".

Paralelo al trabajo en estas áreas, Karisma (Colombia) y Conexión Segura (Venezuela) han trabajado de cerca y tienen vasta experiencia en la documentación y análisis de censura de contenidos, bloqueo de redes y fallas de internet en contextos de efervescencia social y represión.

En Colombia, Karisma acompañó un caso ante la Corte Constitucional para acceder a información pública sobre un corte de internet generalizado en Cali en una de las jornadas más intensas del paro nacional de 2021. Los hechos nunca fueron investigados por el gobierno del entonces presidente Iván Duque (Karisma, 2023). Por esta razón, junto con otras organizaciones de defensa de la libertad de expresión, Karisma ingresó un pedido a la corte para aclarar la situación (Botero & Parra, 2022). La Corte no determinó si la suspensión generalizada del servicio guardaba correlación o no con las protestas. Sin embargo, sí señaló al Estado por incumplir su rol al no haber iniciado investigaciones que aclararan los hechos en su momento.

En contextos en que la censura es más directa, como en el caso de Venezuela, las iniciativas en favor de la libertad de navegación y expresión en línea deben incluir otros enfoques. Conexión Segura busca la promoción y divulgación de herramientas básicas

de seguridad, a través de la difusión de material amigable que enseña a las personas, por ejemplo, a cómo usar un VPN para visualizar sitios que en Venezuela pudieran estar bloqueados, como sitios noticiosos. Justamente con ese fin, este año lanzaron una aplicación para dispositivos Android: Noticias sin Filtro (Conexión Segura, 2024).

5. LECCIONES APRENDIDAS

CONFORMACIÓN DE UN OBSERVATORIO REGIONAL

En más de tres años de trabajo, en un enorme esfuerzo de articulación de las organizaciones adscritas, bajo condiciones cambiantes y con una carga abrumadora en su trabajo diario, OLAD ha logrado poner sobre la mesa algunos de los rasgos comunes en torno al estado de los derechos humanos en el espectro digital en América Latina. El trabajo en conjunto ha permitido estrechar lazos de confianza entre organizaciones muy diversas y con distintos frentes de lucha.

El resultado de esto es un esfuerzo colectivo interseccional por entender, desde una mirada regional, los aspectos clave de cara a la defensa de derechos en línea: amenazas a la democracia o a la libertad de prensa y expresión, el abuso estatal y la violencia de género son solo algunas de las formas en las que se puede ver a la tecnología siendo utilizada como elemento coercitivo por parte de actores maliciosos.

Ya la articulación de un grupo de estas características ha sido un reto enorme, como también lo fueron los procesos de discusión que llevaron a la identificación de patrones comunes en la región y que finalmente condujeron a la redacción de este informe.

El mayor desafío, sin embargo, ha sido la implementación de un sistema que permita medir o cuantificar los resultados del trabajo conjunto entre las distintas organizaciones, lo que en este informe se llamó “reporte de casos propios”. Es un proceso que, al igual que la conformación de OLAD en años anteriores, requiere una adaptación en tiempo real a las necesidades de las organizaciones que lo conforman.

La creación de un observatorio regional de amenazas digitales es una tarea compleja y la coordinación de trabajo común mientras se desarrollan paralelamente las agendas

individuales de cada organización representa un gran desafío que deberá ser analizado en el próximo período de trabajo del Observatorio. Es importante señalar que la amplia gama de características de las organizaciones que forman parte hace que la medición cuantitativa sea más compleja, por lo que este informe recomienda adoptar modificaciones y adaptaciones metodológicas con miras a superar estos obstáculos.

Al mismo tiempo, hay aspectos de la metodología que deben replicarse y que, inclusive, pueden ampliarse con el propósito de recopilar información más segmentada, que ayude a caracterizar a tipos de agresión, víctimas, el perfil de los agresores y el tipo de tecnologías utilizadas para vulnerar derechos. Este es el caso, por ejemplo, de los datos producidos por organizaciones dedicadas a abordar y atender la violencia basada en género en el espacio digital.

Por lo tanto, se entiende que es una necesidad para los próximos ciclos de OLAD identificar en qué áreas de estudio conviene adaptar procesos cualitativos y en qué áreas, por el contrario, es necesario profundizar la medición cuantitativa.

REFLEXIONES SOBRE PERÍODO ANALIZADO

Este informe permite concluir que algunos de los principales actores amenazantes de personas defensoras de derechos humanos son gobiernos, grupos antiderechos que amenazan la libertad de expresión en línea, actores criminales que hacen presencia en el ciberespacio y personas particulares que, mediante expresiones de sexismo y racismo estructural, afectan principalmente a mujeres y personas LGBTIQ+. La ausencia de respuestas estatales es casi una constante y un factor transversal en la región. Destaca además una tendencia al alza de adopción de políticas y estrategias autoritarias por parte de varios gobiernos de la región, que agrega una capa adicional de vulnerabilidad a la población victimizada.

En medio de una ola de criminalidad nunca antes vista en la región (Crisis Group, 2023), se nota una presencia cada vez mayor de actores criminales involucrados en violaciones de derechos en el espectro digital. Un ejemplo de ese tipo de dinámicas es el uso de un sistema de geolocalización de un organismo estatal por parte de un líder criminal en Ecuador para vigilar al candidato presidencial asesinado Fernando Villavicencio. La idea de que un grupo criminal organizado pueda acceder, en tiempo real, a datos personales sensibles de los ciudadanos enciende una alarma regional, pues lo que ocurre en Ecuador podría ya estar ocurriendo en otros países.

En cuanto a vigilancia y espionaje, se observa una tendencia cada vez mayor a la adopción de tecnologías de este tipo. Dichas tecnologías son cada vez más accesibles, especialmente para gobiernos locales. En el caso de spyware más sofisticado como Pegasus, también se ve un patrón regional cuando, mientras este informe se redactaba, el presidente de Colombia Gustavo Petro verificaba una supuesta compra irregular del spyware durante el gobierno de su predecesor, Iván Duque (El Espectador, 2024).

Colombia se convierte así en el quinto país latinoamericano del que se tiene registro de uso del software junto con México, El Salvador, Panamá y República Dominicana. Este informe recomienda actualizar la metodología de trabajo en esta área, quizás hacia una dirección cualitativa, para hallar mecanismos de medición del trabajo de las organizaciones desde una mirada regional.

Varios países de la región, por otro lado, enfrentan grandes desafíos con la desinformación electoral y política. Brasil, por ejemplo, intenta introducir discusiones sobre el rol de las plataformas sociales en la democracia, con el abordaje hacia la desinformación como prioridad. El Estado brasileño se ha enfrentado al poderoso lobby de grandes compañías tecnológicas en esa senda. En Bolivia, bajo una extrema polarización a raíz de la ruptura de su partido oficialista, la desinformación está ganando espacios con mayor fuerza en poblaciones rurales indígenas. En Colombia, la lucha contra la desinformación ha sido caldo de cultivo de numerosas propuestas legislativas, ninguna aprobada hasta ahora, que peligrosamente incluyen mecanismos de censura y que ponen en riesgo el ecosistema digital.

Al igual que la afectación a una infraestructura crítica, como un oleoducto o un banco, las amenazas informáticas a las que se enfrentan personas, comunidades y organizaciones defensoras de los derechos humanos y de la naturaleza, suponen una vulneración grave de sus derechos. Este tipo de agresiones dejan una afectación no solo personal, sino colectiva, pues suponen un ataque a la raíz del ordenamiento democrático de sus países. Desde ese precepto parte la visión de OLAD, que busca dar una respuesta latinoamericana de resiliencia a los fenómenos digitales violentos que aquejan a su población, recibidos desde varios frentes.

6.REFERENCIAS BIBLIOGRÁFICAS

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