INFORME DE POLÍTICA TECNOLÓGICA

Los vigilantes en la mira: Tecnologías de vigilancia para el control político en Venezuela

Andrés Azpúrua · Iria Puyosa

VE SIN FILTRO

DFRLab

VE SIN FILTRO

CONEXIÓN SEGURA Y LIBRE

Sobre VE sin Filtro / Conexión Segura y Libre

VE sin Filtro es un programa dedicado al monitoreo y documentación de amenazas al ejercicio de los derechos humanos en el entorno digital en Venezuela, creado por la organización de derechos humanos digitales Conexión Segura y Libre. Desde 2014, ha rastreado y ayudado a evadir la censura en internet, siendo pionero en la región. Con evidencia técnica y análisis de datos, expone y documenta el alcance de los bloqueos y la censura en internet, la vigilancia gubernamental indiscriminada y los ciberataques contra la sociedad civil. VE sin Filtro ha podido atribuir ataques digitales contra la sociedad civil del gobierno de Venezuela. VE sin Filtro utiliza mediciones de red, análisis técnicos e investigaciones basadas en fuentes abiertas para examinar las restricciones a los derechos humanos en línea y atribuir ataques digitales patrocinados por el Estado en Venezuela. Mediante evidencia técnica y un monitoreo constante, expone y documenta el alcance de los bloqueos y la censura en Internet, la vigilancia gubernamental indiscriminada y los ciberataques contra la sociedad civil.

Conexión Segura y Libre ofrece asistencia de emergencia a organizaciones de la sociedad civil, periodistas y medios independientes que estén siendo atacados o hayan sido bloqueados, ayudando a resolver el incidente y mitigar el impacto de la censura. También brinda soporte y capacitación a activistas, periodistas y organizaciones, y elabora recomendaciones y mejores prácticas para contrarrestar las amenazas contra sus derechos y su seguridad.

Atlantic Council
TECHNOLOGY PROGRAMS

DFRLab

Acerca del Laboratorio de Investigación Forense Digital

El Laboratorio de Investigación Forense Digital (DFRLab) del Atlantic Council es una organización pionera con experiencia técnica y en políticas sobre desinformación, tecnologías conectivas, democracia y el futuro de los derechos digitales. Incubado en el Atlantic Council en 2016, el DFRLab es un constructor de campo que estudia, define e informa los enfoques hacia el ecosistema global de información.

Autores

Andrés Azpúrua, director ejecutivo, Conexión Segura y Libre

Iria Puyosa, investigadora sénior residente en la Iniciativa de Democracia y Tecnología del Atlantic Council

Colaboradores

Daniela Alvarado Mejías, periodista de investigación

Carlos Guerra, asesor técnico en seguridad de la información

Marco Antonio Ruiz, coordinador de comunicaciones, Conexión Segura y Libre

Valentina Aguana, coordinadora técnica de proyectos, Conexión Segura y Libre

Traducción

Laura Vidal

Versión 1.0 - Publicación pública

Portada: Imagen del fallecido presidente venezolano Hugo Chávez en las pantallas del centro de monitoreo del Sistema Integrado de Monitoreo y Asistencia (SIMA) en Caracas, 11 de diciembre de 2013. REUTERS/Carlos Garcia Rawlins

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

Marzo de 2026

Tabla de contenidos

Resumen ejecutivo

Con este informe ofrecemos un análisis detallado de las tecnologías de vigilancia que han sido usadas durante el gobierno de Nicolás Maduro y que continúan aún hoy bajo la administración de la presidenta encargada, Delcy Rodriguez. A pesar del cambio de liderazgo, que tuvo lugar luego de destitución de Maduro por parte de las fuerzas estadounidenses el 3 de enero de 2026, la extensa infraestructura de vigilancia –que cuenta con sistemas de monitoreo en video, intercepción de telecomunicaciones, ciberpatrullaje y ciberataques– continúa estando completamente operacional. El informe documenta asimismo cómo este aparato de vigilancia, que ha costado más de mil millones de dólares, permite la expansión de sistemas integrales de control autoritario que facilitan la represión sistemática de unas 27 millones de personas.

Hallazgos clave

- **Infraestructura de videovigilancia:** La infraestructura de CCTV de Venezuela se ha convertido de modo sistemático, no en una herramienta para la seguridad pública, sino en un arma para el control político. Los proveedores, compañías chinas –en particular CEIEC, Hikvision y Dahua– dominan la cadena de suministro a pesar de las sanciones internacionales. Las capacidades avanzadas de reconocimiento facial y detección de matrículas, reforzadas además con inteligencia artificial, operan sin protección de la privacidad, supervisión judicial ni mecanismos de consentimiento ciudadano. El sistema de respuesta a emergencias VEN911 integra extensas redes de cámaras, lo que permite la rápida identificación y localización de disidentes, manifestantes y opositores políticos. La cooptación de sistemas en municipios liderados por la oposición demuestra hasta qué punto las infraestructuras independientes de seguridad están infiltradas con el fin de afianzar la vigilancia.
- **Vigilancia con drones y monitoreo de movimiento**: Las fuerzas de seguridad venezolanas despliegan un uso sofisticado de drones, combinando sistemas técnicos avanzados con tácticas de guerra psicológica. Drones comerciales operan sin marcos legales que regulen su despliegue o supervisión, desde modelos compactos DJI para usuarios regulares hasta otros más avanzados de Autel con capacidades de vigilancia extendidas. La visibilidad deliberada de las operaciones con drones, en particular con vuelos nocturnos en zonas de protesta y residenciales en las que viven figuras de la oposición, cumplen un doble propósito: recopilar información sobre patrones de movimiento y al mismo tiempo crear un efecto disuasorio y de intimidación para evitar que se tengan reuniones con fines políticos. Los dispositivos de rastreo GPS que fueron descubiertos en vehículos de familiares de presos políticos y que contaban con funciones de escucha revelan el uso de capas de vigilancia encubierta que proporcionan datos continuos de ubicación y audio ambiental.
- **Aplicaciones impulsadas por el Estado:** El “Sistema Patria” constituye una muestra reveladora del uso de plataformas digitales al servicio del control ciudadano. Con este sistema, una herramienta se transformó un recurso para la asistencia social para la extracción sistemática de datos y la manipulación política. La base de datos del Sistema Patria permite la identificación integral y la recopilación de datos a gran escala. Además, su dominio está registrado a nombre del PSUV (el partido de gobierno de Venezuela) y no bajo ninguna agencia del Estado, lo que demuestra hasta qué punto están integrados de modo operativo el aparato estatal y la estructura del partido. El acceso a los beneficios sociales está, además, condicionado al registro obligatorio y al suministro continuo de información personal. Así, el diseño técnico del sistema permite mapear las relaciones de los usuarios con otras personas e instituciones, lo que permite a quienes administran la plataforma crear redes de conexión detalladas incluso de personas no usuarias. En paralelo, la aplicación VenApp se está utilizando de modo explicito para facilitar la delación sistemática de actividades críticas al gobierno.

- **Ciberpatrullaje y vigilancia de redes sociales:** El ciberpatrullaje sistemático a través de distintas plataformas de redes sociales y aplicaciones de mensajería, coordinada por los servicios de inteligencia política y militar SEBIN (Servicio Bolivariano de Inteligencia Nacional) y DGCIM (Dirección General de Contrainteligencia Militar), se ha convertido en una maquinaria integral de persecución digital que criminaliza la expresión en línea. La llamada "Operación Tun Tun" de 2024 fue, además, el ejemplo de cómo se integraron múltiples vías de vigilancia en mecanismos coordinados para la persecusión: funciones de denuncia en VenApp, grupos de doxeo en Telegram, campañas de intimidación en Instagram y arrestos de puerta a puerta. Los procesos penales derivados del ciberpatrullaje se apoyan en contenido digital descontextualizado, sin análisis técnico-forense, procedimientos adecuados de cadena de custodia ni pruebas de daño concreto.
- **Intercepción de telecomunicaciones a gran escala:** La intercepción de telecomunicaciones es el componente más intrusivo del aparato de vigilancia de Venezuela, con evidencia documentada de prácticas sistemáticas que exceden con creces cualquier justificación legítima de aplicación de la ley. El Informe de transparencia 2021 de Telefónica España reveló 1.523.363 líneas de telefonía móvil afectadas y 205.800 órdenes de intercepción, lo que demuestra una vigilancia a escala industrial que es imposible de justificar mediante investigaciones criminales específicas. La infraestructura estatal de CANTV proporciona acceso directo a datos de telecomunicaciones y capacidades de vigilancia del tráfico de Internet. Las deficiencias estructurales del marco regulatorio facilitan el abuso: el mandato del Código Procesal Penal que exige que las instituciones de telecomunicaciones mantengan disponibilidad 24/7 para procesar solicitudes de intercepción, sumado a la subordinación del sistema judicial al poder ejecutivo y la ausencia de supervisión independiente, crea las condiciones para una vigilancia ilimitada sin restricciones significativas.
- **Ciberataques e infiltraciones auspiciados por el Estado:** Los ciberataques con el Estado como impulsor principal son sistemáticos y emplean técnicas sofisticadas que combinan capacidades técnicas con la coordinación entre múltiples entidades gubernamentales. Campañas de phishing a gran escala sabotearon iniciativas de oposición al gobierno como Voluntarios por Venezuela y Héroes de la Salud, además de unidades de organización electoral de base, conocidas como los Comanditos. Algunas campañas de phishing masivo hicieron uso de una manipulación sofisticada de las redes de CANTV para dirigir usuarios a servidores maliciosos controlados por el gobierno. Además, se vulneraron plataformas de la oposición y se utilizaron las capacidades de intercepción de telecomunicaciones para el robo de cuentas. La coordinación entre entidades estatales con mandatos técnicos y regulatorios, y redes anónimas de desinformación revela actividades maliciosas apoyadas por el Estado. Los persistentes esfuerzos de Venezuela por adquirir software comercial espía de múltiples compañías, combinados con la identificación por parte de Citizen Lab de la infraestructura de comando y control de FinFisher en Caracas, apuntan a un despliegue de software de este tipo.
- **Registros e incautaciones de dispositivos sin orden judicial:** La inspección de teléfonos móviles sin orden judicial se ha convertido en una práctica generalizada que combina control, intimidación, castigo y extorsión, en abierta contradicción con las normas nacionales e internacionales de derechos humanos. Los casos reportados revelan cooperación forzada acompañada de coerción y amenazas de detención o procesamiento penal. La extorsión económica agrava el uso de armas políticas, con informes que documentan exigencias de miles de dólares en efectivo o transferencias via Zelle como condición para esquivar detenciones. Personas de alto perfil pueden ser sometidas a inspecciones de equipos en aeropuertos, durante las cuales se pueden llevar a cabo análisis forenses. Algunos patrones emergentes incluyen búsquedas en línea de los nombres de viajeros en Google y redes sociales para encontrar información sobre las opiniones políticas de ciudadanos comunes.

Puntos relevantes

La infraestructura de vigilancia de Venezuela opera como un sistema de control autoritario de amplio alcance que trasciende tecnologías individuales y actores institucionales. La convergencia de la videovigilancia con la intercepción de telecomunicaciones, de ciberpatrullaje con búsquedas en dispositivos, así como aplicaciones patrocinadas por el Estado y los ciberataques, crean una severa restricción del espacio cívico. La existencia en paralelo de varios sistemas de vigilancia crea efectos que se multiplican más que meramente sumarse entre sí. Una persona que asiste a una protesta se enfrenta a múltiples riesgos simultáneos, como la identificación mediante cámaras de reconocimiento facial, la intercepción de

comunicaciones relativas a la organización, la revisión de dispositivos en puestos de control o alcabalas y ciberataques potenciales que pueden comprometer cuentas digitales. Esta vulnerabilidad en varias capas transforma la participación política, protegida constitucionalmente, en actividades de alto riesgo que requieren medidas de seguridad operativas. Las violaciones de derechos humanos van mucho más allá de los abusos inmediatos y causan un profundo daño social, incluyendo la normalización de la autovigilancia y la erosión del espacio cívico.

Es fundamental apuntar que la infraestructura de vigilancia sigue operativa e intacta a pesar de la destitución de Maduro el 3 de enero de 2026. Esto demuestra que las capacidades tecnológicas y los marcos institucionales para el control autoritario trascienden el cambio de liderazgo. Se requiere un desmantelamiento deliberado en lugar de un mero cambio de cabeza en el régimen. Comprender estos sistemas en toda su complejidad —incluyendo las capacidades técnicas, las cadenas de suministro, los operadores institucionales, los marcos legales y las repercusiones en los derechos humanos— resulta esencial para apoyar a la sociedad civil venezolana, que opera en condiciones de severa represión. Es necesario fundamentar respuestas políticas internacionales que aborden tanto los abusos actuales como los futuros mecanismos de rendición de cuentas y que, en última instancia, contribuyan al desmantelamiento del aparato de vigilancia estatal en sí mismo, una condición necesaria para una auténtica transición democrática.

Recomendaciones

El informe ofrece recomendaciones específicas para cuatro grupos de interés y se centra en las necesidades operativas inmediatas de los sujetos más vulnerables al aparato de vigilancia de Venezuela.

- **Para organizaciones de la sociedad civil:** Implementar y brindar capacitación y recursos personalizados en materia de seguridad digital y antivigilancia a poblaciones vulnerables. Crear redes de respuesta de emergencia para brindar asistencia inmediata cuando los activistas enfrenten detención o confiscación de dispositivos. Exigir responsabilidades a los proveedores de tecnología de vigilancia; y establecer mecanismos de seguimiento e intercambio para facilitar la documentación de esta tecnología y sus impactos en los derechos humanos.
- **Para activistas por la democracia venezolana:** Adoptar protocolos de mitigación de la seguridad y vigilancia digital de acuerdo con sus roles y actividades. Usar plataformas de comunicación cifradas de extremo a extremo e implementar autenticación de dos factores basada en hardware para protegerse contra la intercepción de telecomunicaciones. Implementar también protocolos de limpieza de dispositivos para escenarios de alto riesgo, como puestos de control, aeropuertos, protestas y detenciones.
- **Para gobiernos democráticos:** Exigir el desmantelamiento de la infraestructura de vigilancia política. También la rendición de cuentas por los abusos documentados, condicionando el alivio de las sanciones y la cooperación económica a reformas concretas en materia de vigilancia y al enjuiciamiento de funcionarios responsables de violaciones sistemáticas de derechos humanos. Apoyar la capacidad de seguridad digital de la sociedad civil venezolana mediante flujos de financiación específicos, programas de asistencia técnica y de apoyo en infraestructura. Liderar iniciativas multilaterales que establezcan normas contra las exportaciones de tecnología de vigilancia a regímenes autoritarios mediante marcos coordinados de control de las exportaciones y requisitos de transparencia en la cadena de suministro.
- **Para organizaciones multilaterales internacionales:** Desarrollar marcos de rendición de cuentas para proveedores de tecnología de vigilancia que posibilitan violaciones de derechos humanos. Esto mediante la investigación de las cadenas de suministro, la documentación de elementos tecnológicos que hayan facilitado abusos documentados y la búsqueda de mecanismos legales propios al derecho internacional abocado a la protección de los derechos humanos. Brindar asistencia técnica a las organizaciones de la sociedad civil venezolana facilitando el acceso a herramientas de seguridad digital y el desarrollo continuo de capacidades. Coordinar campañas internacionales de promoción dirigidas a las empresas de tecnología de vigilancia a través de foros multilaterales y presión pública; e integrar asimismo las preocupaciones en materia de vigilancia a un monitoreo más amplio de los derechos humanos, asegurando que los mecanismos tradicionales de documentación incorporen sistemáticamente las violaciones de los derechos digitales y la represión habilitada por la tecnología en las investigaciones e informes.

Introducción

En el volátil contexto de la encrucijada venezolana, la organización Conexión Segura y Libre, en conjunto con el Laboratorio de Investigación Forense Digital (DFRLab) del Atlantic Council han elaborado este informe, que examina las tecnologías de vigilancia en el país y su uso para el control político. La destitución de Nicolás Maduro de la presidencia venezolana no se ha traducido en la desmantelación de la infraestructura autoritaria que se construyó durante las últimas dos décadas. El sofisticado aparato de vigilancia —que incluye sistemas de videovigilancia, intercepción de telecomunicaciones, rastreo de redes sociales, aplicaciones digitales estatales, registros e incautaciones de dispositivos, vigilancia con drones y ciberataques— sigue operativo bajo el gobierno interino de Delcy Rodríguez. Comprender estas tecnologías, sus capacidades y su impacto en los derechos humanos es crucial, especialmente en un momento en el que Venezuela atraviesa una transición incierta que podría conducir, bien a una reforma democrática, bien a la consolidación de un Estado de vigilancia bajo una nueva figura de autoridad.

Con este informe ofrecemos un análisis exhaustivo de las tecnologías de vigilancia desplegadas en Venezuela para el control social y político. El análisis abarca tanto las capacidades de vigilancia masiva que afectan a amplios segmentos de la población, como el monitoreo selectivo de individuos y grupos específicos, en particular aquellos involucrados en periodismo, activismo y en la oposición política. El ecosistema de vigilancia que hemos examinado incluye el sistema de respuesta a emergencias VEN911 integrado con redes de circuito cerrado de televisión (CCTV) reconocimiento facial, sistemas de reconocimiento de matrículas, intercepción de telecomunicaciones a gran escala, monitoreo de redes sociales y ciberpatrullaje, aplicaciones móviles configuradas desde el Estado como el Sistema Patria y VenApp; registros sistemáticos e incautaciones de dispositivos electrónicos en puestos de control y centros de detención, así como operaciones de vigilancia con drones y sofisticados ciberataques que incluyen campañas de phishing y un probable despliegue de software malicioso.

El informe documenta las capacidades técnicas de estos sistemas, identifica a los proveedores de tecnología y las cadenas de suministro que los habilitan, mapea su despliegue geográfico en el territorio venezolano, analiza los actores institucionales autorizados para acceder y utilizar datos de vigilancia, y evalúa los impactos en los derechos humanos de la población.

Objetivos

El proyecto tiene tres objetivos principales.

El primero, documentar y analizar las prácticas de vigilancia en Venezuela, ofreciendo una perspectiva de los mecanismos específicos, las capacidades técnicas y el alcance total de las tecnologías implementadas. Esta documentación aborda una brecha crítica de conocimiento acerca de cómo funciona esta maquinaria. La falta de información precisa impide que las poblaciones vulnerables como periodistas, activistas y mujeres en la vida pública implementen medidas efectivas de seguridad digital para mitigar los riesgos y protegerse. Al exponer las prácticas de vigilancia y las cadenas de suministro, el proyecto permite a la sociedad civil, y potencialmente a organismos internacionales, exigir responsabilidades a los proveedores de tecnología por violaciones de derechos humanos.

En segundo lugar, el informe busca proporcionar información para desarrollar esfuerzos para la prevención y medidas de protección para las personas en mayor riesgo. Los hallazgos de la investigación se traducen en ideas basadas en evidencia que orientan acciones concretas de protección contra la vigilancia y la represión. Al proporcionar información y orientación personalizadas, el proyecto puede capacitar a beneficiarios directos en una mejor compresión de las amenazas específicas, a fin de que puedan desarrollar estrategias de seguridad y protección digital más efectivas. Una mejor comprensión de las prácticas de vigilancia del régimen beneficia significativamente a quienes operan en entornos de alto riesgo, permitiéndoles gestionar y contrarrestar mejor las amenazas.

En tercer lugar, fomentar la resiliencia entre las poblaciones vulnerables mediante la sensibilización y la capacidad de acción ciudadana para evadir, desafiar y resistir las prácticas de vigilancia que violan sus derechos. El proyecto busca asimismo fomentar la resiliencia digital no solo entre los beneficiarios directos, sino también entre la población en general, y contribuir de este modo a que en el largo plazo se fortalezcan las instituciones democráticas y la capacidad de la sociedad civil para operar eficazmente a pesar de las presiones de la vigilancia. Esta visión a largo plazo comprende lecciones aplicables a los dos escenarios posibles: el de democratización y el de la supervivencia del regimen autoritario.

Metodología

La investigación empleó múltiples metodologías para garantizar hallazgos exhaustivos y verificables. El análisis técnico de las aplicaciones gubernamentales, en particular la aplicación de Patria, evaluó permisos de recopilación y métodos de almacenamiento de datos para entender vulnerabilidades de privacidad, así como las capacidades de vigilancia estatal. También se utilizaron técnicas de investigación de inteligencia de fuentes abiertas (OSINT) recopiladas y verificadas sistemáticamente, así como información difundida en anuncios gubernamentales accesible públicamente, registros de adquisiciones, publicaciones en redes sociales de las fuerzas de seguridad e investigaciones periodísticas.

Conexión Segura y Libre llevó a cabo una campaña colectiva (que tuvo limitaciones por cuestiones de seguridad) para documentar el despliegue de cámaras de CCTV en toda Venezuela y hacer un mapeo del alcance y la naturaleza de la infraestructura de vigilancia en el país. Mediante el análisis de documentos, Conexión Segura y Libre y DFRLab examinaron marcos legales, registros legislativos, contratos de adquisición, documentos internos filtrados e informes oficiales para comprender el entorno regulatorio que facilita la vigilancia. Además, el equipo de investigación identificó discrepancias entre las políticas públicas oficiales y las prácticas reales.

Se llevaron a cabo entrevistas en profundidad con personas expertas en tecnología y fuentes relacionadas con seguridad, así como con personas que pasaron por experiencias de detención que brindaron testimonios de primera mano sobre patrones operacionales y sobre los impactos de la vigilancia. Las entrevistas siguieron rigurosos protocolos de seguridad para proteger a fuentes en condiciones de alto riesgo. El equipo de investigación también revisó documentación existente de organizaciones de la sociedad civil venezolana, organismos internacionales de derechos humanos y periodismo de investigación independiente para contextualizar los hallazgos dentro de patrones más amplios de control autoritario.

Estructura del informe

El informe está organizado en siete secciones que examinan distintos componentes de la infraestructura de vigilancia en Venezuela.

La primera sección analiza los sistemas de videovigilancia, incluyendo el contexto político y el marco regulatorio que rigen las implementaciones de CCTV; estudios de caso detallados sobre redes de vigilancia en tres áreas urbanas, reconocimiento facial y de matrículas, patrones de acceso y uso por parte de las fuerzas de seguridad, además de riesgos e impactos en los derechos humanos. La segunda sección examina la vigilancia con drones y rastreadores GPS, incluyendo el marco regulatorio, proveedores y capacidades clave de los modelos utilizados; operaciones con drones por parte de las fuerzas de seguridad, despliegues más recientes contra la población civil y los impactos de estas prácticas en los derechos humanos.

La tercera sección analiza las aplicaciones digitales auspiciadas y administradas por el Estado y brinda análisis técnico y documentación de los usos políticos tanto de la aplicación de Patria como VenApp. La cuarta sección investiga las redes sociales y la vigilancia en Internet, abordando las limitaciones a la libertad de expresión en el marco legal, las operaciones de ciberpatrullaje de las instituciones estatales, el acoso y el doxeo de disidentes, las campañas de persecución que encuentran su mejor ejemplo en la "Operación Tun Tun"; y la intersección entre las operaciones de información, la vigilancia y la represión.

La quinta sección evalúa la intercepción de telecomunicaciones privadas, abarcando la base técnica de la intercepción, el marco regulatorio que autoriza la vigilancia, la evidencia de intercepción de telecomunicaciones a gran escala y también los procesos institucionales y las agencias que realizan la intercepción. La sexta sección examina los ciberataques, la infiltración y el software malicioso, abarcando campañas de phishing dirigidas a periodistas y activistas pro democracia, con análisis de objetivos, procedimientos y casos destacados, incluyendo los ataques a Voluntarios por Venezuela y Héroes de la Salud, así como unidades de organización electoral de base (los comanditos). La sección documenta asimismo la intersección entre las operaciones de información y los ataques de phishing. La séptima sección documenta el registro e incautación de dispositivos electrónicos, examinando el contexto político y legal que posibilita estas prácticas; los patrones de registro en puestos de control o alcabalas y aeropuertos; durante detenciones breves, y también la extracción forense empleada por las fuerzas de seguridad.

A lo largo del análisis, el informe se centra en una realidad fundamental: si bien el liderazgo político en Venezuela puede haber cambiado drásticamente con la destitución de Maduro, la infraestructura de vigilancia que permite el control autoritario permanece intacta y operativa. Comprender estos sistemas, sus capacidades y sus impactos en los derechos humanos es esencial para apoyar a la sociedad civil venezolana, orientar las respuestas políticas internacionales, y en última instancia, contribuir a las condiciones necesarias para una auténtica transición democrática.

La evidencia presentada en este informe sirve a múltiples actores: activistas y periodistas que buscan protegerse; autoridades relacionadas con la elaboración de políticas que evalúan las respuestas a la crisis política de Venezuela; empresas de tecnología que evalúan su complicidad en abusos de derechos humanos; y la comunidad internacional que trabaja para apoyar las aspiraciones democráticas de Venezuela.

Contexto: Venezuela ante una nueva promesa de democracia

El 3 de enero de 2026 las Fuerzas Especiales de Estados Unidos llevaron a cabo una operación militar en la base militar Fuerte Tiuna de Venezuela y capturaron a Nicolás Maduro para llevarlo a Estados Unidos a fin de comparecer por cargos ante la justicia de ese país. Esta operación puso fin al régimen autoritario de trece años de Maduro y alteró significativamente la política venezolana. También planteó interrogantes sobre el futuro del país.

A pocas horas de la operación, la entonces vicepresidente, Delcy Rodríguez, asumió como presidente encargada, con lo que se inició un período políticamente inestable marcado por intereses contrapuestos, entre ellos los de Washington DC, los de las facciones internas del chavismo y los que vienen de la sociedad civil venezolana, que demanda una transición democrática.

El enfoque de la administración de Donald Trump hacia la Venezuela post-Maduro priorizó los intereses económicos y estratégicos de Estados Unidos por sobre la promoción de la democracia.[2] Tras la captura de Maduro, el presidente Trump desestimó explícitamente su apoyo a María Corina Machado, Premio Nobel de la Paz 2025 –quien lideró la oposición democrática– y a Edmundo González Urrutia, ampliamente reconocido como el legítimo ganador de las elecciones presidenciales de julio de 2024. Trump enfatizó los intereses de Estados Unidos en el petróleo y los minerales estratégicos venezolanos, manteniendo al mismo tiempo las relaciones con la estructura de poder existente en Venezuela. El 5 de marzo el Departamento de Estado de EEUU publicó un comunicado anunciando el reestablecimiento de las relaciones diplomáticas y consulares, rotas desde el 24 de enero de 2019.[3]

El secretario de Estado de EEUU, Marco Rubio, describió un cronograma de tres etapas para la Venezuela post-Maduro, que incluye la estabilización, la recuperación económica y la eventual transición democrática.[4] Se espera que el cronograma se mida en meses o incluso años. Delcy Rodríguez, por su parte, enfrenta una situación desafiante tratando de equilibrar las demandas de Washington, mantener el control sobre una coalición del chavismo dividida, y gestionar además las complejas relaciones de Venezuela con sus aliados autoritarios. [5]La exigencia del gobierno de Trump a Venezuela de romper vínculos con China, Rusia, Irán y Cuba ha generado desafíos operativos inmediatos. Cabe destacar que los sistemas de vigilancia detallados en este informe son fundamentales para la estabilidad del régimen. Las empresas chinas desempeñan un papel crucial en la infraestructura que sustenta el Estado de vigilancia de Venezuela. Al 20 de marzo de 2026, esta infraestructura de vigilancia permanece plenamente operativa bajo el mandato de Rodríguez, lo que permite al régimen mantener los mecanismos de control social que caracterizaron la era de Maduro. Expulsar a las empresas tecnológicas chinas perturbaría significativamente los sistemas de vigilancia de Venezuela, esenciales para el control interno del régimen.

En mayo de 2025 Rusia firmó un Tratado de Asociación y Cooperación Estratégica con Venezuela que compromete a las dos naciones a una amplia cooperación en hidrocarburos y tecnología militar.[6] Hasta finales de 2025 Rusia fue el principal proveedor de nafta y diluyentes de Venezuela, aditivos esenciales para el procesamiento de los crudos pesados venezolanos. Sin embargo, los acuerdos energéticos firmados el 7 de enero de 2026, que permitieron a Estados Unidos convertirse en el proveedor de diluyentes de Venezuela, entraron en conflicto directo con los compromisos de Rusia. [7]En consecuencia, los funcionarios venezolanos abandonaron con reticencia su asociación de dos décadas con Rusia.[8]

Irán proporciona a Venezuela una importante cooperación internacional relacionada con los intereses de seguridad de Estados Unidos, particularmente en la producción de tecnología de drones en la Base Aérea El Libertador, donde personal iraní ha establecido operaciones de manufactura.[9] El 30 de diciembre de 2025 el Departamento del Tesoro de Estados Unidos impuso sanciones a Empresa Aeronáutica Nacional SA por sus asociaciones comerciales con compañías iraníes involucradas en la producción de drones, recursos que representan una amenaza directa a los intereses estadounidenses. [10]Durante una audiencia en el Senado de Estados Unidos, el Secretario de Estado, Marco Rubio, afirmó que los drones iraníes en Venezuela representan una “línea roja” que Rodríguez debe atender.[11]

Numerosos asesores de inteligencia cubanos se habían integrado a los servicios de seguridad venezolanos, ofreciendo experiencia en contrainteligencia, capacitación en interrogatorios y asistencia en la coordinación de la represión. Hacia el final de enero de 2026 se informó que casi dos mil efectivos cubanos abandonaron Venezuela.[12] Sin embargo, se desconoce el número exacto de personal de seguridad cubano que aún se encuentra en Venezuela, lo que dificulta estimar el impacto en las capacidades de espionaje del régimen.

Tanto el G2 cubano como las fuerzas de inteligencia iraníes estaban vinculadas al aparato de seguridad de Venezuela a través del Centro Estratégico para la Seguridad y Protección de la Patria (CESPPA).[13] El CESPPA se creó en octubre de 2013 como el organismo central de coordinación de inteligencia de Venezuela, con autoridad legal para centralizar la información de todos los servicios de seguridad del Estado (SEBIN, DGCIM y las fuerzas policiales) y declarar confidencial cualquier información que considerara sensible para la seguridad nacional. El 9 de febrero de 2026 la presidente encargada Delcy Rodríguez suprimió y disolvió formalmente el CESPPA mediante el Decreto 5.248, publicado en la Gaceta Oficial Extraordinaria No. 6.985, como parte de un desmantelamiento más amplio de las estructuras institucionales de la era chavista. Esta medida refleja, al menos en parte, la retirada acelerada de la influencia cubana e iraní de Venezuela tras la captura de Maduro y bajo la presión directa de Estados Unidos. La eliminación del CESPPA es la reforma institucional más significativa de la arquitectura de inteligencia de Venezuela en más de una década.[14]

Los primeros pasos hacia la liberalización política en Venezuela se han centrado principalmente en la liberación de presos políticos, con estimaciones que oscilan entre mil y dos mil presos a principios de 2026. Al 19 de marzo del mismo año, la organización venezolana de derechos humanos Justicia, Encuentro y Perdón informó que 679 personas habían sido excarceladas y que al menos 689 estaban aún en privación de libertad, según sus propios registros.[15] La detención continua de personas incluye no solamente a actores políticos, periodistas y personas defensoras de derechos humanos, sino también a ciudadanos y ciudadanas comunes que fueron arrestados por participar en protestas pacíficas o actividades de organización electoral. Entre las personas detenidas se encuentran adolescentes, personas mayores de setenta años (quienes, según la legislación venezolana, deberían estar en arresto domiciliario incluso si son condenadas), personas con enfermedades potencialmente mortales y personas con discapacidad. Cabe destacar que una persona falleció bajo custodia en enero de 2026.[16]

Más allá de las excarcelaciones, otros indicadores de liberalización política siguen siendo mínimos. El aparato de censura venezolano sigue operando a plena capacidad, con 206 sitios web bloqueados, incluyendo 65 medios de comunicación, así como plataformas de redes sociales como X y aplicaciones de mensajería como Signal. Las herramientas para evadir la censura, como las VPN (como NordVPN, Psiphon, Mullvad, TorGuard, Tor Project, Proton) y servidores DNS públicos como Google Public DNS y Cloudflare, también están bloqueados.[17]

El marco legal que permite la criminalización de la disidencia —incluidas la Ley Contra el Odio y la Ley Orgánica Contra el Bloqueo Imperialista— sigue plenamente vigente. Sin embargo, a pesar de la amenaza de arresto, el 12 de febrero de 2026 estudiantes universitarios organizaron manifestaciones pacíficas concurridas en todo el país para recordar a quienes fueron asesinados en protestas anteriores contra el régimen y exigir la liberación de las personas aún en prisión por motivos políticos. Estas fueron las manifestaciones más grandes registradas en el país desde la represión de agosto de 2024, durante la cual al menos veinticinco personas fueron asesinadas, decenas sufrieron breves desapariciones forzadas y alrededor de 2400 fueron detenidas arbitrariamente.[18]

Al momento de editar este informe, María Corina Machado y Edmundo González Urrutia aún no pueden regresar de modo seguro a Venezuela. El continuo exilio de estos líderes venezolanos, electos democráticamente, obstaculiza significativamente cualquier transición democrática pues su ausencia física impide organizar actividades políticas o ejercer el mandato otorgado por sus electores.

En el período post-Maduro ha surgido una tensión fundamental: si bien la destitución de Maduro eliminó a la figura principal del régimen, la infraestructura autoritaria que ha sustentado dos décadas de represión política permanece vigente y operativa. Comprender esta infraestructura, en particular el extenso aparato de vigilancia descrito en este informe, es crucial para evaluar el potencial de una transición democrática frente a la continuación de un régimen autoritario bajo un nuevo liderazgo.

Sistemas de videovigilancia

El extenso sistema de videovigilancia desplegado en Venezuela sirve como herramienta de control interno. Este aparato opera dentro de un vacío legal que prácticamente no protege el derecho a la privacidad de los ciudadanos ni las garantías del debido proceso. Si bien la incorporación de los sistemas de CCTV a las políticas de seguridad pública data de 2007, su expansión significativa comenzó en 2013 cuando el entonces ministro de Interior, Justicia y Paz, Miguel Rodríguez Torres, anunció una inversión de 1.200 millones de dólares para instalar 30.000 cámaras en 16 ciudades a través de un acuerdo con la Corporación de Importación y Exportación de Electrónica de China (CEIEC).[19] Esta iniciativa creó el Sistema Integrado de Monitoreo y Asistencia (SIMA), junto con el sistema de emergencia VEN911. En 2019 la Gran Misión Cuadrantes de Paz reorganizó las políticas de seguridad en torno a pequeños sectores territoriales con patrullajes fijos, manteniendo el monitoreo centralizado a través de VEN911..[2120]

El régimen aceleró drásticamente el despliegue de CCTV a lo largo de 2025 bajo la dirección del actual Ministro del Interior, Diosdado Cabello. En junio de 2025 el comandante de VEN911, Neptalí Rodríguez, reportó 3.920 cámaras operativas monitoreadas a través de 26 Centros de Comando, Control y Telecomunicaciones, incluída la sede nacional, 19 oficinas estatales y seis instalaciones municipales.[22] Para diciembre de 2025 Cabello anunció que la cifra había aumentado a aproximadamente 7.000 cámaras, lo que representa un aumento del 78,6% en solo seis meses. [23]Esta expansión coincidió con la exhortación de Cabello, en noviembre de 2025, de "cubrir la mayor parte del territorio con cámaras" y su directiva de que los alcaldes presionaran a las empresas privadas para que reorientaran sus cámaras de seguridad hacia las vías públicas, lo que hace que esta infraestructura de vigilancia comercial sea integrada a las redes estatales de monitoreo. El ministro reconoció explícitamente el 3 de abril de 2025 que "el 911 está distribuido por toda Venezuela y está enlazado con las cámaras que tienen los centros comerciales [y] los conjuntos residenciales", lo que revela la integración entre sistemas de seguridad en principio privados y el aparato de inteligencia nacional.[24]

La ola de despliegue de 2025 extendió la vigilancia más allá de los espacios públicos tradicionales a hospitales, barrios residenciales y bastiones de la oposición. El 22 de junio de ese año, la entonces ministra de Salud, Magaly Gutiérrez, anunció la instalación de cámaras en los principales hospitales para monitorear a los pacientes y al personal médico, enmarcando la vigilancia como necesaria para prevenir "sabotaje" por parte de elementos de la oposición no especificados.[25] La alcaldesa de Caracas, Carmen Meléndez, anunció el 15 de agosto de 2025 sus planes de instalar "cámaras inteligentes" en cada semáforo y esquina de la capital, amenazando explícitamente con fotografiar y procesar a los ciudadanos por infracciones menores como tirar basura en la calle. "Si vemos a alguien desde el puesto de comando lanzando la basura a las calles, le vamos a sacar la fotico, lo vamos a buscar y posteriormente le vamos a aplicar la Ordenanza de Convivencia Ciudadana, Civismo y Justicia de Paz Comunal" declaró Meléndez en agosto de 2025 durante una entrevista radial.[26]

Lo más significativo es que Cabello reconoció el 16 de julio de 2025 que las cámaras de seguridad jugaron un "papel clave en la identificación de los manifestantes" durante las manifestaciones post-electorales que tuvieron lugar del 29 de julio al 3 de agosto de 2024, confirmando públicamente lo que las organizaciones de la sociedad civil habían documentado previamente: que las imágenes de CCTV permiten la identificación, seguimiento y detención de personas críticas al gobierno de manera sistemática. Esta agresiva expansión ocurrió precisamente cuando se intensificó la represión política tras las fraudulentas elecciones de julio de 2024, lo que sugiere que el despliegue de infraestructura de vigilancia contribuye directamente a la consolidación del régimen y no a la seguridad ciudadana. Hoy, el gobierno de Delcy Rodríguez hereda esta repotenciada capacidad técnica.

Es probable que VEN911 tenga un propósito mucho más amplio que simplemente responder a emergencias de seguridad pública, dada su huella de implementación observada y la arquitectura técnica de su infraestructura, proporcionada por el fabricante chino de telecomunicaciones ZTE. Además, dado que se cuenta con al menos once centros de comando operacional, organizados en una clara jerarquía nacional-regional-estatal, el sistema tiene la infraestructura física para permitir un monitoreo continuo de la población en áreas urbanas, particularmente en Caracas y otras ciudades importantes.

Entre los sistemas que componen VEN911, la característica principal del servicio Smart City Solution de ZTE es su integración con plataformas de análisis de volúmenes masivos de datos e inteligencia artificial. Se alinea con las capacidades que han sido reconocidas por las autoridades venezolanas: identificación retroactiva de manifestantes a partir de grabaciones, rastreo de matrículas en los puntos de acceso a la ciudad y transmisión en tiempo real a los centros de comando.[27] Además, el servicio Government Cloud Solution, también de ZTE, proporciona un elemento habilitante crucial: una plataforma de datos unificada e interdepartamental. [28]Esto significa que los datos de vigilancia recopilados a través de las cámaras VEN911 pueden cruzarse con el registro Patria, las bases de datos del SEBIN y los registros de intercepción de telecomunicaciones de otras agencias del régimen. La combinación de estos sistemas desarrollados por ZTE indica que VEN911 podría tener la capacidad de rastrear continuamente el movimiento de personas de interés e identificar retrospectivamente a los participantes de reuniones públicas. Estas capacidades superan las de un sistema convencional de despacho de emergencias y constituyen la columna vertebral operativa del aparato de vigilancia política del régimen.

La ausencia de mecanismos de supervisión judicial, políticas de retención de datos o controles de acceso permite que estos sistemas se utilicen como arma contra disidentes, manifestantes y organizaciones de la sociedad civil con impunidad. Esta sección examina tres despliegues notables, analiza la cadena de suministro detrás de la infraestructura y evalúa las implicaciones para los derechos humanos bajo el régimen gobernante, ahora encabezado por Delcy Rodríguez.

Implementaciones de CCTV

Tres despliegues ilustran los diversos modelos operativos, la dinámica política y las implicaciones para los derechos humanos que caracterizan la infraestructura de CCTV de Venezuela. La Gran Caracas ejemplifica la arquitectura de vigilancia más sofisticada del régimen, en la que el sistema nacional VEN911 se integra con las redes municipales para crear capacidades integrales de monitoreo en toda la región capitalina. El estado Trujillo demuestra cómo los recursos del gobierno nacional financian la expansión de la vigilancia en las regiones del interior del país en condiciones que priorizan los objetivos de seguridad del régimen sobre la seguridad ciudadana, algo visible en la instalación de cámaras concentrada en instalaciones gubernamentales y en las oficinas del partido gobernante, el PSUV. La ciudad de Los Teques, en el municipio de Guaicaipuro del estado Miranda, representa el despliegue de vanguardia del régimen, que combina las capacidades avanzadas de inteligencia artificial de Hikvision, incluyendo reconocimiento facial y detección de matrículas. Además, los elogios del ministro Cabello al sistema por su capacidad para “detectarlo todo” e “identificar a quienes buscan actuar con impunidad” [29] le suman a esto mensaje político explícito. En conjunto, estos casos exponen cómo la infraestructura de vigilancia, que según se había dicho sería para prevenir el delito, se convirtió en un arma para el control autoritario.

Área Metropolitana de Caracas: Cooptación de los sistemas municipales de seguridad pública

La región capitalina alberga la infraestructura de CCTV más extensa de Venezuela, integrando los sistemas VEN911 con las redes municipales de cinco municipios. Funcionarios de inteligencia informan que la sede de VEN911 en Plaza Venezuela mantiene centros de comando con señal directa de cámaras estratégicamente ubicadas que monitorean las principales vías públicas, incluyendo las principales avenidas y autopistas de la ciudad. El sistema incluye instalaciones fijas y unidades de comando móviles equipadas con conjuntos de cámaras desplegables en postes extensibles.

El municipio Libertador, administrado directamente por el gobierno nacional por estar ubicado en la capital del país, sirve como campo de pruebas para arquitecturas de vigilancia centralizada. Según Neptalí Rodríguez, para junio de 2025 había 774 cámaras de seguridad en el municipio. Desde octubre de 2024 los proyectos de instalación de cámaras en la zona han sido gestionados por la Fundación Caracas Inteligente, que funciona bajo la dependencia de la Alcaldía de Caracas.[30] Entre los proyectos que han implementado se encuentran la instalación de redes Wi-Fi en espacios públicos, así como botones de pánico y cámaras de seguridad vinculadas al VEN911 y a los sistemas de los Cuadrantes de Paz . En sus redes sociales, la Fundación Caracas Inteligente ha informado sobre la instalación de cámaras en plazas públicas como la Plaza de la Victoria y Plaza Venezuela, y también en terminales de autobuses como el Terminal de La Bandera y el terminal de tránsito rápido Ruta 421 en el centro de Caracas. [31]También se instalaron quince paradas de autobús “inteligentes” en toda la ciudad, equipadas con botones de pánico y

cámaras vinculadas a los sistemas de VEN911 y a los sistemas de los Cuadrantes de Paz. T[32]anto las cámaras como los botones de pánico instalados por la Fundación Caracas Inteligente fueron fabricados por la empresa china Hangzhou Hikvision Digital Technology Co., actualmente sancionada por Estados Unidos y la Unión Europea por desarrollar software de detección de "personas clave" que ha sido usado para vigilar a minorías étnicas en China.[33]

Cámaras Hikvision ubicadas en el sector Plaza Venezuela del municipio Libertador. (Fuente: Caracas Inteligente en Instagram [34])

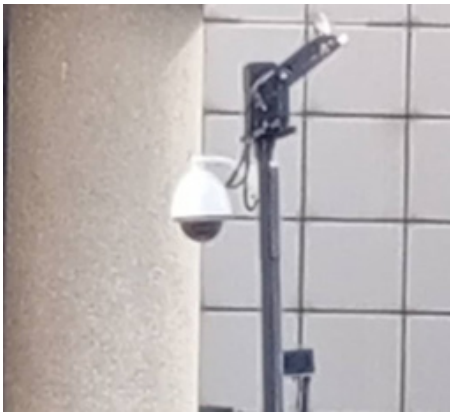
Los municipios liderados por la oposición en el estado Miranda enfrentan presiones complejas con respecto a la infraestructura de vigilancia. En municipios como Chacao, Baruta y El Hatillo se han desarrollado sistemas paralelos que en principio están dedicados a la seguridad pública legítima, y que oficialmente operan de forma independiente, pero que enfrentan presiones persistentes para integrarse con el aparato de seguridad nacional. Estos municipios ejemplifican un patrón más amplio en el que una infraestructura de seguridad aparentemente independiente es cooptada para la represión política. Estos sistemas locales también plantean riesgos para activistas de la oposición, manifestantes y críticos del régimen, porque el gobierno central puede solicitar y obtener acceso a sus sistemas de cámaras.

El municipio Chacao es un ejemplo de esta doble dinámica: su Centro de Seguridad y Comunicación Integrada (CISC) emplea equipos Hikvision y el software HikCentral Professional V3.0 para gestionar una amplia cobertura de cámaras en todo municipio y su importantes espacios comerciales. En marzo de 2024 Chacao instaló diez botones de emergencia que permiten la comunicación directa por video con operadores del CISC. El municipio promocionó estas instalaciones como mejoras de seguridad pública, pero su integración en bases de datos nacionales centralizadas sigue siendo opaca. Residentes y activistas por los derechos de las mujeres denuncian una mayor vigilancia en zonas en las que tradicionalmente las mujeres organizan iniciativas comunitarias y protestas.

El alcalde de Chacao, Gustavo Duque, ha destacado el sistema de vigilancia de su municipio como “el más moderno del país”, con tecnología de reconocimiento facial y detección de matrículas.[35] En sus redes sociales, el alcalde ha mostrado que las cámaras pueden enfocar claramente detalles a más de cien metros de distancia. Hay al menos 310 cámaras activas en este pequeño municipio de casi 13 kilómetros cuadrados, con una densidad de población moderadamente alta de aproximadamente 3. personas por kilómetro cuadrado.[36]34Estas cámaras son administradas por el CISC, que trabaja en conjunto con la Policía Municipal de Chacao. El CISC cuenta con un protocolo para la detección inmediata de “eventos anómalos” –como manifestaciones– que permite la activación de controles de monitoreo específicos y la coordinación de despliegues en tiempo real. Existen indicios de coordinación operativa entre el CISC y el sistema VEN911, pero no hay evidencia de integración técnica. El CISC ha desactivado temporalmente las cámaras en lugares específicos cuando se realizan procedimientos como redadas u operaciones de organismos como la Dirección General de Contrainteligencia Militar (DGCIM) para evitar que estos eventos queden registrados en sus sistemas.

Estas cámaras son administradas por el CISC, que trabaja en conjunto con la Policía Municipal de Chacao. El CISC cuenta con un protocolo para la detección inmediata de “eventos anómalos” –como manifestaciones– que permite la activación de controles de monitoreo específicos y la coordinación de despliegues en tiempo real. Existen indicios de coordinación operativa entre el CISC y el sistema VEN911, pero no hay evidencia de integración técnica. El CISC ha desactivado temporalmente las cámaras en lugares específicos cuando se realizan procedimientos como redadas u operaciones de organismos como la Dirección General de Contrainteligencia Militar (DGCIM) para evitar que estos eventos queden registrados en sus sistemas.[37]

En julio de 2022 activistas en Chacao hicieron grafittis con lemas de la oposición cerca de la avenida Libertador (una importante avenida intermunicipal) y fueron detenidos en cuestión de horas. Organizaciones de la sociedad civil documentaron evidencia que sugiere que las grabaciones de las cámaras de seguridad facilitaron su rápida identificación y arresto. Los activistas detenidos —principalmente hombres y mujeres jóvenes afiliados al partido opositor Voluntad Popular— enfrentaron cargos de “incitación al odio” y “conspiración”. Las activistas denunciaron interrogatorios particularmente invasivos sobre sus relaciones con hombres en sus organizaciones, lo que refleja prejuicios de género sobre la participación de las mujeres en la disidencia política.



Cámara ubicada en el sector de La Castellana del municipio Chacao, Caracas. (Fuente: VEsinFiltro)

En todo el municipio de Chacao pueden verse cámaras PTZ (pan-tilt-zoom) en forma de domo con visión de 360 grados que pueden girar horizontal y verticalmente mientras amplían o reducen la imagen. Todo el sistema opera exclusivamente en una red IP e incluye un grabador digital de video (DVR), que es un sistema de grabación que distribuye la señal de la cámara a tabletas utilizadas por el personal autorizado. El alcalde, así como otros funcionarios y figuras políticas, pueden ver la señal en tiempo real desde sus tabletas.[38]

Cámaras fijas y PTZ Hikvision en el sector Altamira (izquierda) y Los Palos Grandes (derecha) del municipio Chacao. (Source: VEsinFiltro)

Los municipios de Baruta y El Hatillo también mantienen redes de seguridad independientes utilizando equipos Hikvision, pero operan en entornos donde las fuerzas de seguridad nacionales pueden requisar las imágenes de las cámaras sin autorización judicial.

En Baruta existe un centro de coordinación de comando y control VEN911 desde 2016, aunque se desconoce el número exacto de cámaras de seguridad que gestiona. Asimismo, la Alcaldía de Baruta opera de forma independiente su propio sistema de videovigilancia, con cámaras fijas y PTZ distribuidas por todo el municipio. Sin embargo, las autoridades municipales no han revelado información sobre el número de cámaras que operan, su ubicación, o las características de su sala de control.

Sala de monitoreo en el VEN911. Sede Baruta. (Fuente: Ven911baruta en Instagram) [39]

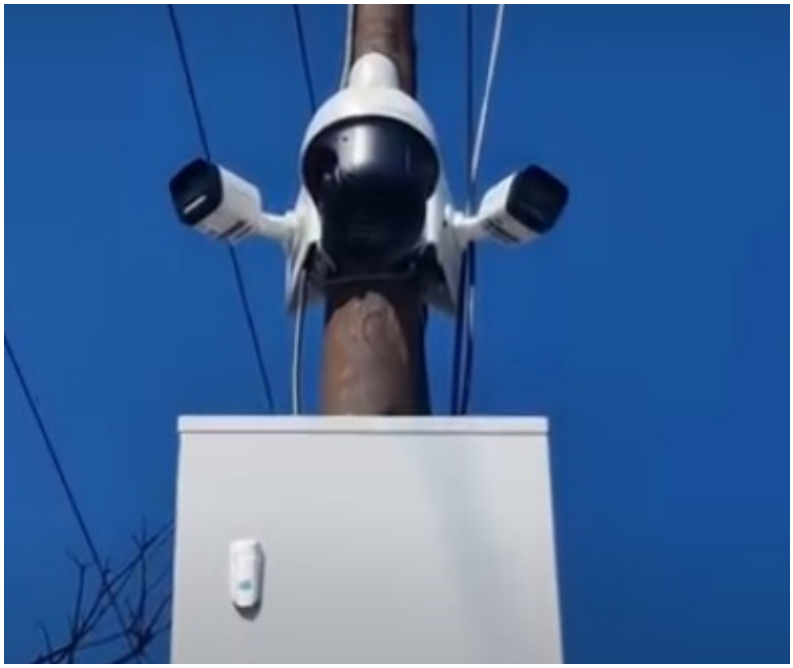
Cámaras del sistema VEN 911 en Chuao, municipio Baruta. (Fuente: VEsinFiltro)

Desde 2021 el municipio El Hatillo ha instalado cámaras de seguridad en lugares como el centro histórico y el sector Los Naranjos. Para agosto de 2023 este municipio de baja densidad poblacional contaba con 30 dispositivos, entre los que se incluyen cámaras PTZ y mini bala. Estas cámaras cuentan con inteligencia artificial y una capacidad de zoom similar a la de los sistemas utilizados en el municipio Chacao. Las cámaras desplegadas en este municipio son administradas por el Centro de Control Integrado (CCI) que a su vez, envía los informes de incidentes al Centro de Operaciones de la Policía Municipal de El Hatillo. Al igual que en Chacao, la alcaldía no ha reconocido públicamente ningún vínculo con VEN911 ni con los Cuadrantes de Paz. Para abordar asuntos de seguridad pública, El Hatillo también utiliza los sistemas de radio de la policía y una red de más de 100 grupos vecinales en WhatsApp. Estos grupos sirven como canales de comunicación directa donde los residentes pueden solicitar información personalizada sobre su zona, presentar quejas y reportar incidentes al CCI.

Múltiples modelos de cámaras de seguridad en El Hatillo, Caracas. (Fuente: PoliHatillo en Instagram38[40])

El SIMA comenzó a operar en el municipio Sucre en 2013 como parte de un proyecto piloto para reducir la delincuencia en los barrios de Petare. El 20 de diciembre de 2025 el Ministro del Interior, Diosdado Cabello, informó que el municipio tenía más de seiscientas cámaras de seguridad operativas, algunas de las cuales fueron ubicadas a lo largo de un tramo de la carretera Gran Mariscal de Ayacucho, que comunica Caracas con la localidad de Guarenas.[41]

Muchas de estas cámaras fueron instaladas por la empresa estatal CANTV, utilizando fibra óptica integrada al sistema VEN911 y a los Cuadrantes de Paz. En este municipio, investigadores de Conexión Segura han observado cámaras antiguas tipo bala, así como cámaras domo y mini bala, fabricadas por Dahua Technology, en barrios marginados como Petare y La Dolorita.



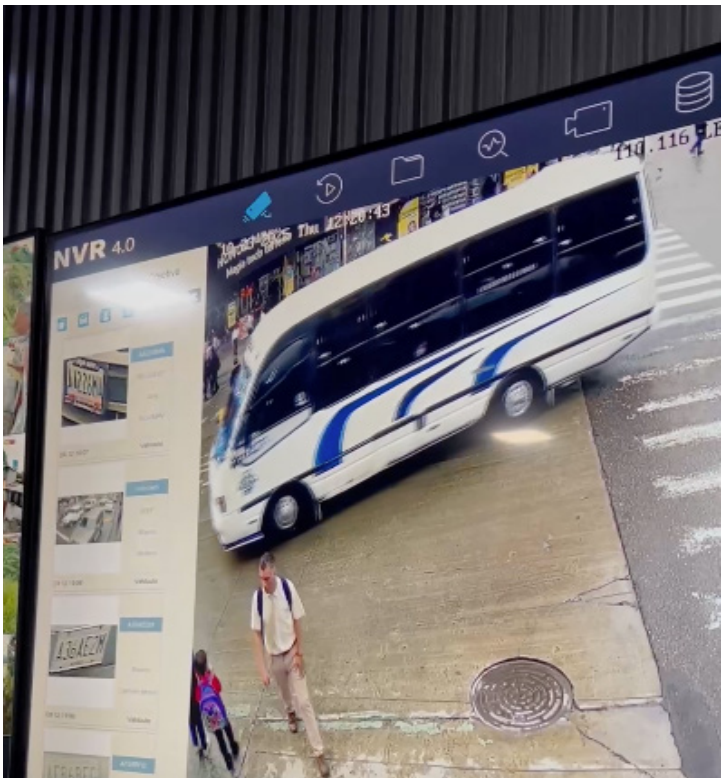
Cámaras instaladas en el municipio Sucre. (Fuente: Cantv_ve en Instagram)

A pesar de la agitación política de enero de 2026, la instalación de cámaras de vigilancia cerca de los lugares de protesta y de interés político sigue en marcha. El 21 de enero las fuerzas de seguridad instalaron nuevas cámaras con vista directa a los campamentos de familiares de presos políticos, quienes organizaban vigilias fuera del centro de detención Zona 7, ubicado en el municipio Sucre, administrado por el PSUV, el partido gubernamental. Las cámaras se instalaron para grabar a los participantes de las vigilias y a quienes se acercaban para brindar apoyo material (alimentos, medicamentos, mantas) a las familias de las personas detenidas. El impacto de género de dicha vigilancia resulta particularmente agudo: las mujeres constituyen la mayoría de los familiares que mantienen estas vigilias y enfrentan mayores riesgos de identificación, acoso y detención.

SOS Guaicaipuro: capacidades avanzadas de inteligencia artificial

La ciudad de Los Teques constituye un despliegue modelo del régimen, combinando una amplia cobertura de cámaras con capacidades avanzadas de inteligencia artificial y mensajes políticos explícitos. En 2022 el alcalde Farith Fraija inició la instalación de cámaras de seguridad en puntos estratégicos de Los Teques para crear un sistema de monitoreo en tiempo real, coordinado con los Cuadrantes de Paz. El proyecto comenzó con veinte cámaras conectadas a una sala situacional de VEN911 a la que llamaron SOS Guaicaipuro.[42] Para el 23 de diciembre de 2025, Fraija anunció que el municipio había alcanzado la instalación de 400 cámaras, cubriendo los principales puntos de acceso de la ciudad, avenidas concurridas, plazas públicas, áreas residenciales y barrios de bajos ingresos.[43]

La trascendencia política del despliegue de Guaicaipuro se hizo explícita el 13 de noviembre de 2025 cuando Cabello visitó Los Teques y elogió efusivamente la infraestructura de vigilancia: “Guaicaipuro tiene un sistema de cámaras extraordinario, porque puede detectarse todo, especialmente en la capital, cualquier lugar y evento, que permite identificar a quienes buscan actuar impunemente, siendo clave para los cuerpos de seguridad”.[44]



Sistema NVR 4.0 utilizado por SOS Guaicaipuro, mostrando su tecnología de reconocimiento de matrículas vehiculares. (Fuente: Farith Fraija, alcalde de Guaicaipuro, en TikTok)[46]

El municipio exhibe abiertamente en redes sociales la sofisticación técnica de su infraestructura suministrada por Hikvision. Todas las cámaras son del reconocido proveedor chino, incluyendo modelos PTZ, de torreta, bala y mini bala, que ofrecen una cobertura integral. En un video del 23 de octubre de 2025 Fraija mostró la Sala de Operaciones de SOS Guaicaipuro, mostrando monitores con la interfaz de firmware NVR 4.0 de Hikvision.[45] Este sistema avanzado emplea inteligencia artificial para el reconocimiento facial, la detección automática de matrículas, el mapeo térmico y el conteo de personas. Fraija destacó explícitamente estas capacidades de IA en materiales promocionales, demostrando la confianza del régimen en que la tecnología de vigilancia avanzada sirve a sus intereses. La sala de operaciones también cuenta con un teclado de red Hikvision DS-1100KI(C) con joysticks de cuatro ejes, que permite a los operadores controlar remotamente las cámaras PTZ para el seguimiento en tiempo real de personas o vehículos.

El despliegue de Guaicaipuro ilustra varias dinámicas preocupantes. En primer lugar, la rápida expansión de 20 a 400 cámaras en tres años demuestra la capacidad del régimen para ampliar la infraestructura de vigilancia a pesar de las limitaciones económicas, lo que sugiere que la vigilancia recibe prioridad presupuestaria sobre servicios sociales. En segundo lugar, la integración explícita de las capacidades de reconocimiento facial en tiempo real y detección de matrículas —tecnologías que las sociedades democráticas regulan rigurosamente— opera sin ninguna protección de la privacidad, supervisión judicial ni mecanismos de consentimiento ciudadano. En tercer lugar, la celebración pública de Cabello de la capacidad del sistema confirma que los funcionarios del régimen consideraban deseable una vigilancia integral y no ven ningún costo político en amenazar abiertamente a los disidentes. En cuarto lugar, la entusiasta promoción del monitoreo con inteligencia artificial por parte del alcalde Fraija sugiere que los funcionarios locales reconocieron que una expansión visible de la vigilancia mejoraba su prestigio.

Estado Trujillo: integración de fuentes informantes

El 26 de abril de 2025 el gobernador Gerardo Márquez y la Ministra de Salud, Magaly Gutiérrez, inauguraron nuevas sedes del centro de mando estatal, que incluyen una sala de monitoreo y videovigilancia para el municipio de Valera con 72 cámaras fabricadas por la empresa china Dahua Technologies.[47] El comando del estado Trujillo interopera con el sistema 1×10 del Buen Gobierno, que recibe los informes de la comunidad enviados a través de Línea 58, una función de VenApp que permite a los usuarios enviar quejas e informes a las autoridades gubernamentales. [48]El sistema se integra con salas situacionales del gobierno ubicadas en cada comuna, responsables de dar seguimiento a los reportes presentados en la plataforma 1x10. Este centro de comando se coordina con el sistema de videovigilancia VEN911 y la aplicación VenApp. Esto implica una conexión entre las agencias gubernamentales que enlazan el sistema de vigilancia con la plataforma de mensajería VenApp, que se ha utilizado para revelar información confidencial de individuos a quienes el régimen etiqueta como “terroristas”.[49]

Cámaras adquiridas en el año 2024 por la Gobernación de Trujillo. (Fuente: gobtrujillo en Instagram) [50]

Durante las ceremonias religiosas de la canonización de José Gregorio Hernández en octubre de 2025, el gobierno estatal reinauguró la sede de la Policía de Trujillo en Isnotú, lugar de nacimiento del santo. El gobernador Gerardo Márquez informó que se instalaron 18 cámaras PTZ como parte de un sistema de videovigilancia en las entradas y salidas, así como en el centro. Es de destacar en este punto que activistas de derechos humanos tomaron la ocasión de la la celebración religiosa para pedir la liberación de presos políticos. El 18 de octubre de 2025 el periodista y exconcejal opositor Yorbin García fue identificado y detenido por agentes del Servicio Bolivariano de Inteligencia Nacional (SEBIN) cerca del Santuario de Isnotú. Conexión Segura no pudo confirmar un vínculo directo entre esta detención y las cámaras instaladas en el pueblo, pues un gran contingente de fuerzas de seguridad, como el SEBIN y la Dirección General de Contrainteligencia Militar (DGCIM), estuvieron presentes y patrullaron constantemente la zona durante la ceremonia.

Suministro de tecnología

Las empresas chinas dominan la cadena de suministro de tecnología de vigilancia de Venezuela, lo que refleja alineaciones geopolíticas más amplias. Comprender las relaciones con los proveedores resulta esencial para evaluar las capacidades técnicas y las posibles vulnerabilidades del sistema de vigilancia que hereda la administración Rodríguez.

Entre 2009 y 2013 se asignaron aproximadamente 80 millones de dólares del Convenio Bilateral Cuba-Venezuela al desarrollo del Centro de Seguridad y Respuesta a Emergencias 171 (CEASE 171), predecesor directo del VEN911, a través del Fondo Nacional de Desarrollo (FONDEN). Cuba participó en proyectos como el Sistema Nacional de Seguridad Ciudadana (SINASEC) y la instalación de 171 centros de respuesta a emergencias en los estados Aragua, Barinas, Falcón, Portuguesa y Trujillo.[51] No obstante, no hay evidencia clara de que alguno de estos proyectos se haya implementado en su totalidad.

Después de 2013 China se convirtió en el principal proveedor de tecnología de vigilancia en Venezuela. La mayoría de las empresas chinas identificadas como proveedoras de tecnologías de vigilancia para Venezuela han sido sancionadas por Estados Unidos, incluidas ZTE Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company y Autel Robotics.[52]

Proveedores chinos

La Corporación de Importación y Exportación de Productos Electrónicos de China (CEIEC por sus siglas en inglés) surgió como el arquitecto principal de la infraestructura de vigilancia centralizada de Venezuela a través de su contrato de 1.200 millones de dólares anunciado en 2013. La compañía reestructuró todo el sistema VEN911 que abarca videovigilancia, despacho de emergencias y análisis de datos.[53] Las unidades de comando móviles con conjuntos de múltiples cámaras desplegables montadas en postes telescópicos son un equipo característico del CEIEC, visible en la cobertura de las operaciones de seguridad por parte de medios estatales.

En 2020 el Departamento del Tesoro de Estados Unidos sancionó a la CEIEC por “apoyar los esfuerzos del régimen ilegítimo de Maduro para socavar la democracia en Venezuela, incluidos los esfuerzos para restringir el servicio de Internet, llevar a cabo vigilancia digital y operaciones cibernéticas contra opositores políticos”.[54] La CEIEC ha estado involucrada en la seguridad penitenciaria venezolana a través del Sistema Tecnológico de Seguridad Penitenciaria (Sitiosep). [55]Las continuas operaciones de la empresa indican mecanismos para evadir sanciones y priorizar las capacidades de vigilancia del régimen a pesar del aislamiento internacional.

Unidad de mando móvil con sistema multicámara CEIEC sobre mástil desplegable. (Fuente:VEsinFiltro)

Hikvision ha captado una cuota de mercado significativa más allá de los contratos con el gobierno nacional, suministrando equipos tanto a redes de seguridad gubernamentales como a redes municipales controladas por la oposición. Hikvision se enfrenta a restricciones de la US Entity List (una lista de restricciones comerciales publicada por el Departamento de Comercio la Oficina de Industria y Seguridad de los EEUU) por su participación en la infraestructura de vigilancia de Xinjiang.[56] La empresa proporciona cámaras, grabadoras de video en red (NVR), DVR y software de gestión a municipios del estado Miranda, incluyendo Baruta, Chacao, El Hatillo y Zamora, todos con alcaldes afiliados al partido Fuerza Vecinal, que no forma parte formalmente de la coalición del régimen chavista. El CISC de Chacao utiliza HikCentral Professional V3.0, una plataforma avanzada de gestión de seguridad que integra múltiples transmisiones de cámaras, sistemas de control de acceso y herramientas de análisis. Hikvision también suministra botones de emergencia instalados en el municipio Chacao que permiten a los usuarios contactar directamente con el CISC por videollamada en caso de emergencia. El modelo utilizado en Chacao corresponde a la estación de alarma de pánico Hikvision DS-PEA2-21. [57]Desde diciembre de 2024 la Fundación Caracas Inteligente también comenzó a instalar este mismo modelo de intercomunicador en varias plazas y lugares estratégicos del municipio Libertador.[58]

Zhejiang Dahua Technology Co., Ltd. se ha convertido en un importante proveedor de hardware para instalaciones de vigilancia pública en Venezuela. Su cámara tipo bala IPC-HFW2541T-ZAS se ha instalado en varios municipios como Caracas, Miranda y Trujillo. Este modelo es una cámara comercial de gama media con óptica varifocal motorizada, visión nocturna infrarroja y análisis de video integrado. Las especificaciones técnicas de la cámara admiten funciones como la detección de intrusiones perimetrales y la clasificación de objetos, con funciones de reconocimiento facial y de matrículas integradas en los flujos de datos de comando VEN911.

Estaciones de alarma en los municipios Chacao (izquierda) y Libertador (derecha). (Fuentes: luisgonzalofer en Instagram; Caracasinteligente en Instagram)

A pesar de haber sido incluida en la US Entity List en octubre de 2019, dada su participación en la vigilancia y represión de las poblaciones uigures en Xinjiang, Dahua ha mantenido el acceso al mercado venezolano.[59]Además, Dahua y la administración venezolana han estado explorando una mayor integración de IA en sus sistemas.

Acuerdos de alto nivel entre China y Venezuela, así como testimonios de trabajadores sobre el terreno, han revelado también la participación de otras empresas chinas como Huawei Technologies Co. Ltd, ZTE Corporation y China CAMC Engineering Co. Ltd en proyectos vinculados al sistema VEN911, aunque el alcance de su participación no está claro.

Proveedores bielorrusos

Entre 2021 y 2023 el Ministerio del Poder Popular para las Relaciones Interiores, Justicia y Paz de Venezuela (MPPRIJP) sostuvo conversaciones con la empresa bielorrusa Synesis para la adquisición de software para mejorar su integración de sistemas de videovigilancia y reconocimiento facial avanzado.[60] Estados Unidos sancionó a Synesis por proporcionar un software utilizado por las autoridades bielorrusas para facilitar la identificación y el arresto de manifestante[61]

El software Kipod ofrecido a Venezuela incluye:

- Sistema de reconocimiento facial, que incluye notificaciones y búsquedas de personas específicas y sus patrones de movimiento.
- Reconocimiento de matrículas.
- Detección de una persona con un arma de fuego/arma blanca.
- Detección de objetos abandonados.
- Detección de humo (una demostración para funcionarios del gobierno utilizó una imagen de protestas en Caracas como ejemplo).
- Detección de multitudes.
- Control de seguridad perimetral y detección de objetos en la zona.
- Monitoreo del cumplimiento de las normas de tránsito.

Un memorando de hoja de ruta se firmó entre el MPPRIJP y 24x7 Panoptes, la subsidiaria de Synesis que opera el sistema de vigilancia en Bielorrusia, durante una reunión intergubernamental en Caracas en 2021.[62] En 2023, durante una visita oficial a una reunión intergubernamental en Minsk, el almirante Juan Carlos Oti, director general de los Centros de Comando, Control y Telecomunicaciones (VEN 911), presenció una demostración del software en la Jefatura de Situación Operativa del Departamento de Policía de la Ciudad de Minsk. Se desconoce si la demostración prevista en Venezuela se llevó a cabo o si se adquirió el software.

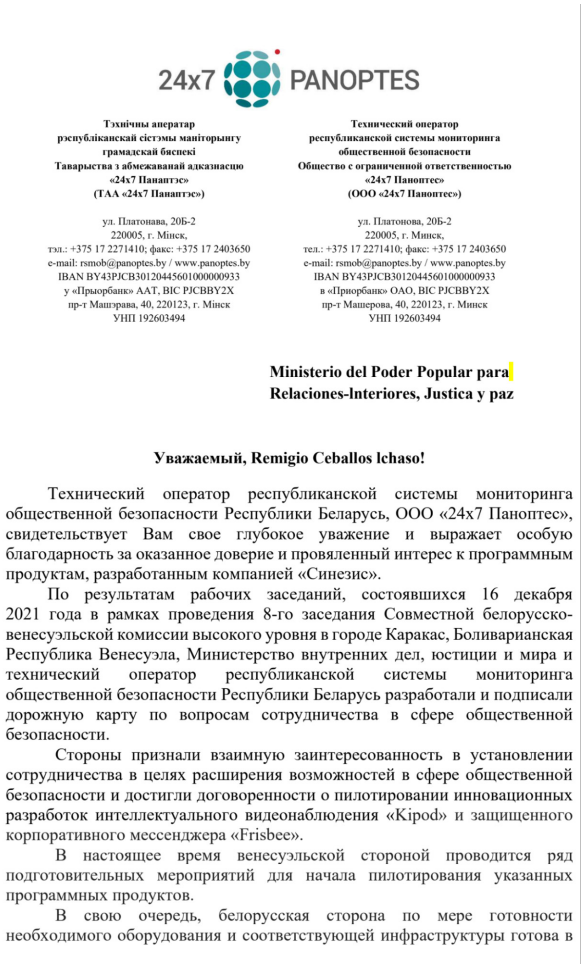
El Almirante Juan Carlos Oti, Director General de los Centros de Comando, Control y Telecomunicaciones (VEN 911) en la Dirección General de Asuntos Internos del Comité Ejecutivo de la Ciudad de Minsk, en 2023. (Fuente: Ministerio del Interior del Comité Ejecutivo de la Ciudad de Minsk) [63]

El acceso y uso de los sistemas de CCTV por parte de las fuerzas de seguridad

El sistema VEN911 parece funcionar como un centro donde las entidades de seguridad nacional pueden acceder a las imágenes de las cámaras, incluido el Servicio Bolivariano de Inteligencia Nacional (SEBIN), la Dirección General de Contrainteligencia Militar (DGCIM) y el Ministerio de Relaciones Interiores, Justicia y Paz. Las fuerzas de seguridad podrían acceder a videos para llevar a cabo investigaciones contra opositores políticos, monitorear protestas, identificar activistas y facilitar operaciones de arresto.

La arquitectura de vigilancia venezolana carece de las salvaguardas fundamentales que emplean los sistemas democráticos para prevenir el abuso. Ningún marco legal regula cómo se pueden usar las grabaciones, quién puede acceder a ellas ni con qué fines. La ausencia de supervisión judicial, políticas de retención de datos, controles de acceso y organismos de supervisión civil crea un entorno donde las fuerzas de seguridad pueden explotar los sistemas de CCTV para la persecución política sin ninguna rendición de cuentas.

Durante una transmisión de su programa de televisión Con el mazo dando del 16 de julio de 2025, Cabello reconoció que las cámaras de seguridad en las calles jugaron un papel clave en la identificación de los manifestantes durante las protestas que tuvieron lugar entre el 29 de julio y el 3 de agosto de 2024, en respuesta al robo de las elecciones presidenciales.bello dijo: “¿Ustedes saben qué hacían los inocentes pobres niños de Atocha de la oposición? Provocaban al policía, lo empujaban, y después se grababan cuando el policía se molestaba y reaccionaba; lo que pasaba antes no salía. Ahora hay cámaras por todos lados, así que pórtense bien, los están viendo, los están mirando.”[64]



24x7 PANOPTES

Тэхнічны аператар
рэспубліканскай сістэмы маніторынгу
грамадскай бяспекі
Таварыства з абмежаванай адказнасцю
«24x7 Панаптэс»
(ТАА «24x7 Панаптэс»)

ул. Платонава, 20Б-2
220005, г. Мінск,
тэл.: +375 17 2271410; факс: +375 17 2403650
e-mail: rsmob@panoptes.by / www.panoptes.by
IBAN BY43PJCB30120445601000000933
у «Прыорбанк» ААТ, BIC PJCBBY2X
пр-т Машэрава, 40, 220123, г. Мінск
УНП 192603494

Технический оператор
республиканской системы мониторинга
общественной безопасности
Общество с ограниченной ответственностью
«24x7 Панаптес»
(ООО «24x7 Панаптес»)

ул. Платонова, 20Б-2
220005, г. Минск,
тел.: +375 17 2271410; факс: +375 17 2403650
e-mail: rsmob@panoptes.by / www.panoptes.by
IBAN BY43PJCB30120445601000000933
в «Приорбанк» ОАО, BIC PJCBBY2X
пр-т Машерова, 40, 220123, г. Минск
УНП 192603494

Ministerio del Poder Popular para Relaciones-Interiores, Justica y paz

Уважаемый, Remigio Ceballos Ichaso!

Технический оператор республиканской системы мониторинга общественной безопасности Республики Беларусь, ООО «24x7 Панаптес», свидетельствует Вам свое глубокое уважение и выражает особую благодарность за оказанное доверие и провяленный интерес к программным продуктам, разработанным компанией «Синезис».

По результатам рабочих заседаний, состоявшихся 16 декабря 2021 года в рамках проведения 8-го заседания Совместной белорусско-венесуэльской комиссии высокого уровня в городе Каракас, Боливарианская Республика Венесуэла, Министерство внутренних дел, юстиции и мира и технический оператор республиканской системы мониторинга общественной безопасности Республики Беларусь разработали и подписали дорожную карту по вопросам сотрудничества в сфере общественной безопасности.

Стороны признали взаимную заинтересованность в установлении сотрудничества в целях расширения возможностей в сфере общественной безопасности и достигли договоренности о пилотировании инновационных разработок интеллектуального видеонаблюдения «Kipod» и защищенного корпоративного мессенджера «Frisbee».

В настоящее время венесуэльской стороной проводится ряд подготовительных мероприятий для начала пилотирования указанных программных продуктов.

В свою очередь, белорусская сторона по мере готовности необходимого оборудования и соответствующей инфраструктуры готова в

Carta del director A. P. Knysh de la empresa bielorrusa 24x7 Panoptes dirigida a Remigio Ceballos, Ministro del Poder Popular para las Relaciones Interiores y Justicia, proporcionada porBELPOL.

El 7 de agosto de 2025, Cabello ofreció una rueda de prensa para anunciar que el Servicio Bolivariano de Inteligencia Nacional (SEBIN) había frustrado un supuesto intento de atentado contra un monumento recientemente inaugurado en la zona de Plaza Venezuela, adyacente a un edificio administrativo del SEBIN. Mostró imágenes tomadas por cámaras de seguridad del lugar donde se ve a un hombre dejando allí una bolsa, en la que supuestamente se encontraron explosivos.[65] El hombre grabado por las cámaras, identificado como José Daniel García Ortega, apareció posteriormente en un video difundido por Cabello en el que confesaba el hecho, vinculando a la oposición venezolana con un supuesto plan para llevar a cabo varios atentados en el país. Un total de 13 personas fueron arrestadas y acusadas de participar en el plan. Los autores intelectuales, de acuerdo con las acusaciones, serían la líder de la oposición María Corina Machado y los ex-presidentes de Colombia Álvaro Uribe, Iván Duque, Andrés Pastrana y Juan Manuel Santos.

Las cámaras de seguridad también se han utilizado para intimidar directamente a manifestantes que participan en manifestaciones pacíficas. El 21 de enero de 2026 familiares de presos políticos recluidos en la comandancia de la Policía Nacional Bolivariana (PNB), conocida como Zona 7, denunciaron la instalación de cámaras de seguridad para monitorear el campamento donde llevaban semanas realizando una vigilia para exigir la liberación de los presos prometida por el rgobierno. En videos compartidos en redes sociales, se puede ver a agentes colocando un trípode con una cámara en el techo de un vehículo antidisturbios. Esta cámara estaba conectada al panel de control de otra cámara ya instalada en un poste cercano.[66] El dispositivo instalado por la policía apuntaba directamente a las carpas donde dormían los manifestantes y a la zona designada como baño. Los agentes argumentaron que la instalación era legal porque estaba ubicada en una zona de seguridad cerca de la sede policial.

Cámaras móviles utilizadas para monitorear a los manifestantes en la Zona 7 en enero de 2026. (Fuente: cristiancrespoj en X) [67]

La información pública sobre las políticas de retención de datos sigue siendo inexistente. Los funcionarios de seguridad entrevistados afirmaron conservar las grabaciones durante períodos que van desde 90 días a seis meses, aunque las prácticas reales probablemente varíen considerablemente. Los centros de comando de VEN911 pueden conservar grabaciones durante períodos más largos, en particular grabaciones de objetivos de alto valor identificados con fines de inteligencia. La capacidad técnica para realizar búsquedas retroactivas (consultar grabaciones de archivo para rastrear los movimientos de un individuo días o semanas después de la grabación) puede suponer graves riesgos para activistas y disidentes. Una vez que las fuerzas de seguridad identifican a una persona de interés, pueden reconstruir sus movimientos históricos, identificar personas asociadas, mapear redes y establecer patrones. Combinadas con datos de intercepción de telecomunicaciones, monitoreo de redes sociales e inspecciones de dispositivos en controles de seguridad, las grabaciones de CCTV podrían permitir una vigilancia exhaustiva de objetivos específicos.

Riesgos e impactos de la videovigilancia en los derechos humanos

Las fuerzas de seguridad pueden utilizar las imágenes de las cámaras de seguridad para identificar a los participantes de las protestas y, posteriormente, detenerlos, hostigarlos y procesarlos. Saber que las fuerzas de seguridad vigilan los espacios públicos mediante extensas redes de CCTV tiene un profundo efecto inhibidor sobre la participación política y la libertad de expresión. Esto lo confirman activistas de base en Caracas. Muchas personas redujeron su presencia en espacios públicos, limitaron las reuniones presenciales o dejaron de organizar actividades abiertas a partir de 2024. Los activistas optaron por reuniones pequeñas, cambios frecuentes de ubicación, uso mínimo de teléfonos móviles y autocensura en redes sociales y grupos comunitarios. Estas personas respondieron a una encuesta sobre el tema y en sus respuestas señalaron la tensión de ser observados constantemente. Las encuestas indican que los venezolanos no perciben los sistemas de CCTV como

herramientas de seguridad pública, sino como dispositivos de control social utilizados para identificar, rastrear y disuadir a los ciudadanos críticos del régimen. En el discurso cotidiano los sistemas de CCTV son denominados como “los sistemas de control”, “las cámaras del partido”, “las aplicaciones para marcar personas” o simplemente “la vigilancia”.

Riesgos del reconocimiento facial

Si bien la implementación integral del reconocimiento facial sigue siendo incierta, la amenaza genera graves impactos psicológicos en disidentes y activistas. Se debe suponer siempre que las fuerzas del orden pueden utilizar las grabaciones extraídas de estos sistemas de CCTV para identificar personas. Las capacidades avanzadas de reconocimiento facial permitirían la identificación en tiempo real de personas en protestas, eventos públicos o incluso en actividades rutinarias como el desplazamiento al trabajo. Combinado con las extensas bases de datos que mantienen las fuerzas de seguridad, el reconocimiento facial permitiría rastrear a prácticamente cualquier persona de interés en espacios públicos.

Al igual que las políticas que rigen el acceso y la conservación de grabaciones, las capacidades de reconocimiento facial de los diversos sistemas de vigilancia no se han hecho públicas. Dependiendo de la combinación de estas políticas y capacidades técnicas, podría ser posible buscar retroactivamente en las grabaciones las acciones y rutas seguidas por una persona de interés, semanas o meses después de su grabación. Otro riesgo, aunque menos probable en el contexto venezolano, es que los operadores de estos sistemas puedan identificar a cualquier persona en el video en tiempo real al cruzar su rostro con bases de datos estatales.

Riesgos de vigilancia a través de matrículas

La proliferación de sistemas de CCTV con reconocimiento de matrículas integrado, junto con lectores de matrículas instalados en rutas estratégicas –como accesos vehiculares a Caracas y carreteras regionales– podría facilitar el rastreo vehicular a gran escala. Esto en particular si están integrados y registran los movimientos de todos los vehículos, no solo una lista de matrículas en específico. Este tipo de rastreo continuo y prácticamente inevitable, sin las garantías suficientes y sin una supervisión judicial efectiva, amenazaría gravemente la libertad de movimiento y el derecho a la privacidad, lo que representaría riesgos para los disidentes.

Vigilancia mediante drones y otros métodos para monitorear el movimiento en espacios públicos

Tras las controvertidas elecciones presidenciales de julio de 2024 y la posterior crisis política, las fuerzas de seguridad venezolanas ampliaron la vigilancia aérea y terrestre dirigida a la movilización de la oposición y las actividades de la sociedad civil. El despliegue de drones de grado industrial, equipados con cámaras de alta resolución, termografía y potentes funciones de zoom, mejoró el monitoreo de protestas, concentraciones políticas y disidentes individuales. Como complemento a esta infraestructura de vigilancia aérea, las fuerzas de seguridad han instalado dispositivos de rastreo GPS con capacidad de escucha en vehículos de familiares de presos políticos y figuras de la oposición. Estas tecnologías de rastreo de ubicación operan de forma encubierta, requiriendo acceso físico a los vehículos en la mira para proporcionar datos completos sobre patrones de movimiento y lugares visitados con frecuencia, lo que permite el rastreo en tiempo real.

Esta sección examina en primer lugar las operaciones de vigilancia con drones dirigidas a protestas y reuniones de la oposición. Luego analiza las tácticas de intimidación que emplean la presencia visible de drones, documenta el despliegue de dispositivos de rastreo GPS y concluye con un análisis de los impactos sobre los derechos humanos en ambas modalidades de vigilancia.

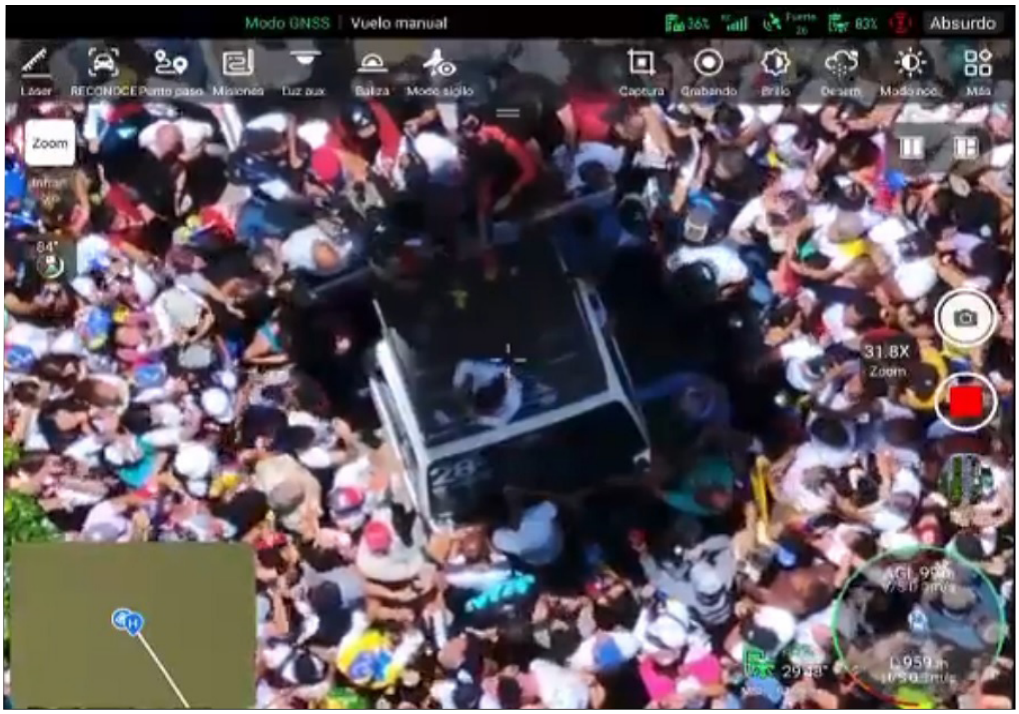
Monitoreo de protestas mediante vigilancia con drones

Los primeros despliegues de drones en Venezuela se originaron a partir de contratos asociados al sistema VEN911. Los drones proporcionados al Ministerio del Interior, Justicia y Paz en virtud de estos contratos tuvieron un despliegue operativo limitado y actualmente parecen no estar operativos; algunas unidades aún son visibles en oficinas e instalaciones de entrenamiento de pilotos.[68]

La crisis post-electoral de 2024 impulsó la expansión de las operaciones de vigilancia con drones. Las fuerzas de seguridad desplegaron drones para vigilar las calles, vigilar las protestas y rastrear a las personas, empleando simultáneamente estas capacidades con fines intimidatorios.[69] Los protocolos para el funcionamiento de drones por parte de las fuerzas de seguridad del Estado siguen sin ser revelados.

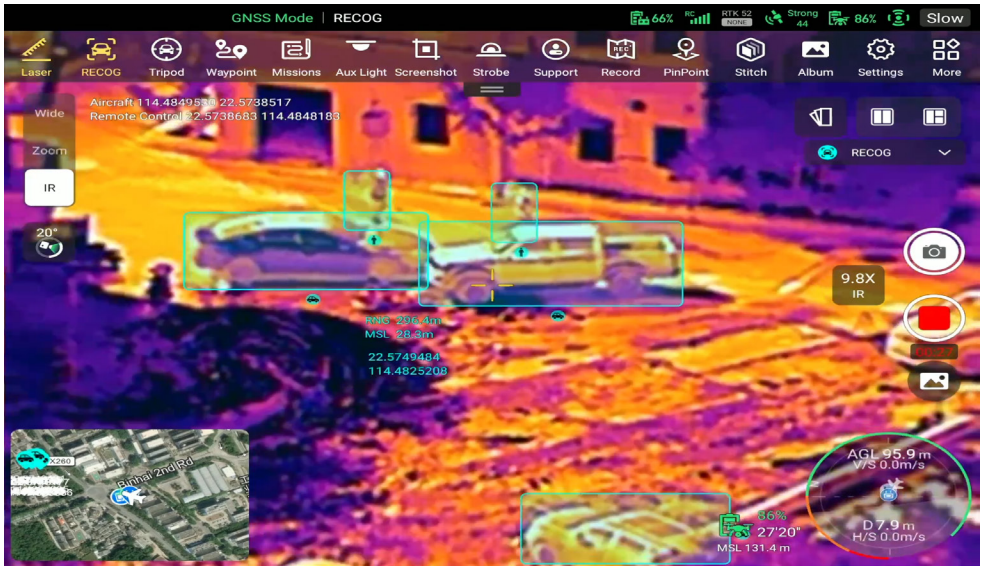
Los drones más sofisticados que fueron identificados son las unidades Autel EVO Max 4T.[70] Este es un modelo corporativo cuadricóptero de vigilancia especializado, con una autonomía de vuelo de hasta 42 minutos y un alcance de transmisión de 20 kilómetros. Su característica más destacada es su versátil sistema de cámara 4 en 1, que incluye una cámara con zoom de 48 MP, un zoom óptico de 10x y un zoom híbrido de 160x, capaz de identificar vehículos a dos kilómetros de distancia. Además, cuenta con una cámara gran angular de 50 MP, una cámara termográfica de 640x512 y un telémetro láser con un alcance de 1.200 metros. El EVO Max 4T está equipado con capacidades autónomas avanzadas, como navegación sin GPS mediante SLAM, red multiunidad A-Mesh, seguimiento de sujetos con IA y resistencia a interferencias electromagnéticas. Autel comercializa esta plataforma específicamente para su uso en vigilancia de seguridad pública, operaciones de búsqueda y rescate, así como monitoreo de infraestructuras. El EVA Max 4T ha sido adquirido y desplegado formalmente en al menos dos zonas de conflicto activo: Ucrania –tanto por fuerzas rusas como ucranianas– y Gaza, por parte de las fuerzas israelíes. Estos despliegues en el campo de batalla dieron como resultado que Estados Unidos añadiera a Autel a la lista de empresas militares chinas de la Sección 1260H del Pentágono en enero de 2025.

El EVA Max 4T ha sido adquirido y desplegado formalmente en al menos dos zonas de conflicto activo: Ucrania –tanto por fuerzas rusas como ucranianas– y Gaza, por parte de las fuerzas israelíes.[71] Estos despliegues en el campo de batalla dieron como resultado que Estados Unidos añadiera a Autel a la lista de empresas militares chinas de la Sección 1260H del Pentágono en enero de 2025.[72]



Zoom 31.8x de María Corina Machado en un mitin captado por un dron. Video publicado por Delcy Rodríguez en X. (Fuente: @delcyrodriguezv en X)

Tras las elecciones presidenciales de 2024 la líder opositora María Corina Machado se convirtió en el principal objetivo de vigilancia. El 3 de agosto de 2024, durante un mitin de la oposición en una zona comercial de Caracas, un dron capturó imágenes de alta resolución que mostraban el rostro de Machado en un primerísimo plano mientras se quitaba la capucha que le cubría el rostro al subir a la plataforma del camión que servía de escenario. A pesar de llegar en motocicleta para evitar ser identificada por las autoridades, el zoom óptico de 31,8x del dron permitió su identificación desde una distancia considerable. La entonces vicepresidente Delcy Rodríguez difundió estas imágenes en redes sociales, demostrando tanto la capacidad de vigilancia como la disposición del régimen a hacer público su monitoreo del liderazgo opositor.[73]



Interfaz de usuario del operador de Autel Alpha con cámara infrarroja habilitada, como se ve en un video promocional del fabricante. (Fuente: Autel Robotics) [74]

VEsinFiltro ha documentado al menos 20 casos distintos de despliegue de drones, principalmente para captar grabaciones aéreas de manifestaciones de la oposición en Caracas y en otras ciudades. Estas grabaciones fueron compartidas en las redes sociales por altos funcionarios del régimen y medios estatales oficiales.[75] Las imágenes mostraron que estos drones podían enfocar nítidamente los rostros de individuos específicos desde la distancia, lo que sugiere que las autoridades podrían usar esta tecnología para identificar y enfocarse en personas que estuviesen participando en la manifestación.

Imagen de promoción para el Autel Alpha con el título de un artículo en el sitio web del vendedor (Fuente: Advexure)[76]

Otros modelos avanzados que fueron identificados como en uso operativo incluyen el Autel Alpha, un modelo corporativo cuadricóptero de vigilancia pesado de 6,34 kg en configuración estándar, que anteriormente no figuraba en los inventarios de las fuerzas de seguridad venezolanas.[77] La Guardia Nacional Bolivariana opera unidades Autel Dragonfish, drones de ala fija de despegue y aterrizaje vertical (VTOL por sus siglas en inglés) diseñados para operaciones prolongadas. La Guardia Nacional mantiene la responsabilidad del control del orden público, lo que hace que estas plataformas de vigilancia de larga duración sean especialmente útiles para monitorear actividades políticas.

Modelo	Fuerzas de seguridad operativas	Tipo
DJI mini 2	GNB	Cuadricóptero compacto de consumo (plegable)
DJU Mini 3	CPNB	Cuadricóptero compacto de consumo (plegable)
DJI Mini 4 Pro	CPNB	Cuadricóptero compacto de consumo (plegable)
DJI Mavic Air 2	GNB, CPNB	Cuadricóptero comercial de consumo (plegable)
Autel EVO Max 4T	SEBIN	Cuadricóptero industrial de vigilancia (plegable, resistente a la intemperie)
Altar Alfa	SEBIN	Cuadricóptero de vigilancia industrial pesado (plegable, resistente a la intemperie)
Autel Swordfish	GNB	Dron de ala fija VTOL industrial, de vigilancia y defensa
DJI AVATA	GNB	Cuadricóptero con vista en primera persona para el consumidor

Tabla con una selección de modelos de drones identificados en uso por la fuerza de seguridad venezolanas. (Fuente: VEsinFiltro.)

Intimidación y acoso mediante la presencia visible de drones

Entre el 30 de julio y el 3 de agosto de 2024 se documentaron en redes sociales la aparición de drones sobrevolando varias zonas del centro de Caracas en horario nocturno. En estas publicaciones, los drones, equipados con múltiples luces, parecían buscar focos de protesta y probablemente sirvieron como táctica de intimidación.

Las imágenes de los drones de vigilancia fueron compartidas en redes sociales por residentes que los observaban desde las ventanas de sus apartamentos en el centro de Caracas. Los analistas indican que las agencias de seguridad que operaban estos drones buscaban infundir miedo y crear un efecto disuasorio entre los posibles manifestantes. Esta opinión se basa en la cantidad de drones que patrullaban el mismo sector simultáneamente, en lugar de desplegarse de forma más dispersa para cubrir áreas más extensas. Además, algunos de los modelos identificados son técnicamente capaces de volar sin luces, pero se observó constantemente que los drones patrullaban con las luces encendidas. Esta decisión no respondía a ninguna necesidad operativa y parece estar diseñada para maximizar la conciencia pública de su presencia, lo que sugiere un propósito intimidatorio.[79]

Además de monitorear protestas, estos drones también podrían usarse para espiar a personas en la disidencia. El 7 de enero de 2025 Machado denunció que drones sobrevolaban la casa de su madre, Corina Parisca, en Caracas.[80] Un incidente similar se reportó el 23 de noviembre de 2024 en la Embajada de Argentina en Caracas, donde cinco personas de la oposición solicitaban asilo. Uno de ellos, Pedro Urru-

churtu, denunció en su cuenta de redes sociales el uso de drones para monitorearlos durante el asedio a la embajada por parte de las fuerzas de seguridad.[81]

El 6 de enero de 2026, pocos días después de que Nicolás Maduro fuera capturado por las fuerzas armadas estadounidenses, se observaron vuelos de drones monitoreando las inmediaciones del Palacio Presidencial de Miraflores y posiblemente otros lugares estratégicos durante la noche. En ese incidente, individuos armados no identificados, partidarios del régimen, reaccionaron con confusión disparando, según se informó, contra los drones de vigilancia estatal, pensando que se trataba de un segundo ataque de las fuerzas estadounidenses.[82]

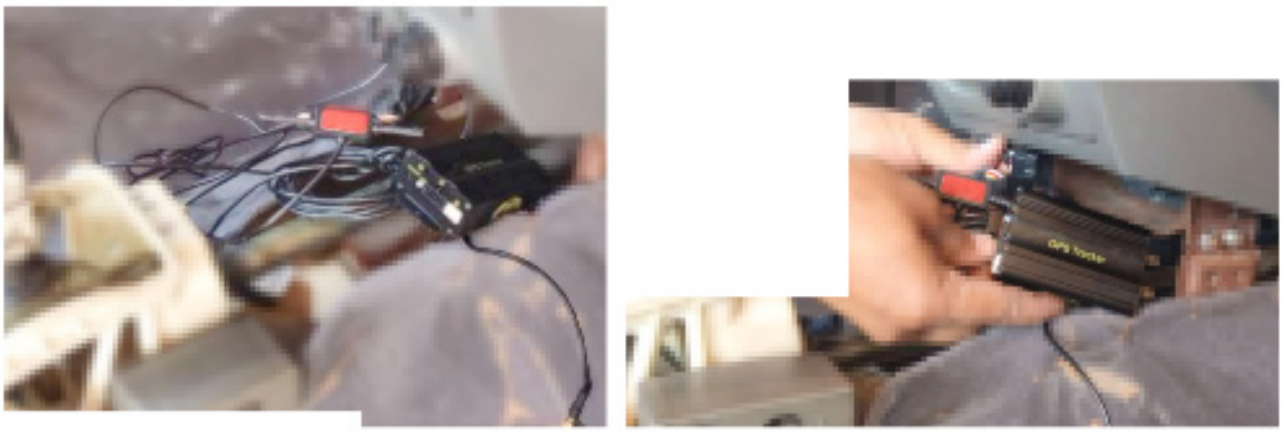
Rastreadores GPS y dispositivos de escucha

La tecnología de rastreo GPS permite la vigilancia encubierta de los movimientos de objetivos durante largos periodos. Su instalación requiere acceso físico al vehículo objetivo en un momento en que el propietario no se percate de la intrusión. Una vez desplegados, los dispositivos de rastreo generan flujos de datos de ubicación casi continuos que los operadores pueden aprovechar para reconstruir rutas, identificar lugares visitados con frecuencia, establecer patrones de movimiento y habilitar el rastreo en tiempo real para facilitar operaciones de vigilancia adicionales. Los dispositivos documentados en operaciones de vigilancia venezolanas incluyen micrófonos integrados que permiten espiar conversaciones. El rastreo GPS resulta necesariamente más riesgoso desde el punto de vista operativo si los operadores desean evitar la detección, pues se requiere acceso físico a los vehículos. Sin embargo, proporciona capas adicionales de vigilancia que aumentan la inmediatez, la granularidad, la resiliencia frente a prácticas anti vigilancia y la capacidad de independencia operativa.

Instancias de rastreo GPS han incluido espionajes dirigidos a vehículos de familiares de presos políticos con antecedentes militares. La focalización en las familias de estos detenidos puede reflejar las preocupaciones de las fuerzas de seguridad sobre las actividades de los familiares de detenidos, o puede formar parte de una estrategia de vigilancia más amplia que apunta a grupos que abogan por la liberación de los presos políticos. También es posible que estas personas hayan sido puestas en la mira porque sus casos son percibidos como particularmente amenazantes para la seguridad del régimen. De acuerdo con las evaluaciones de organizaciones de la sociedad civil, los familiares de ciertos presos políticos civiles u otros actores podría haber sido objeto de un ataque similar sin haberlo sabido.

Rastreadores internos

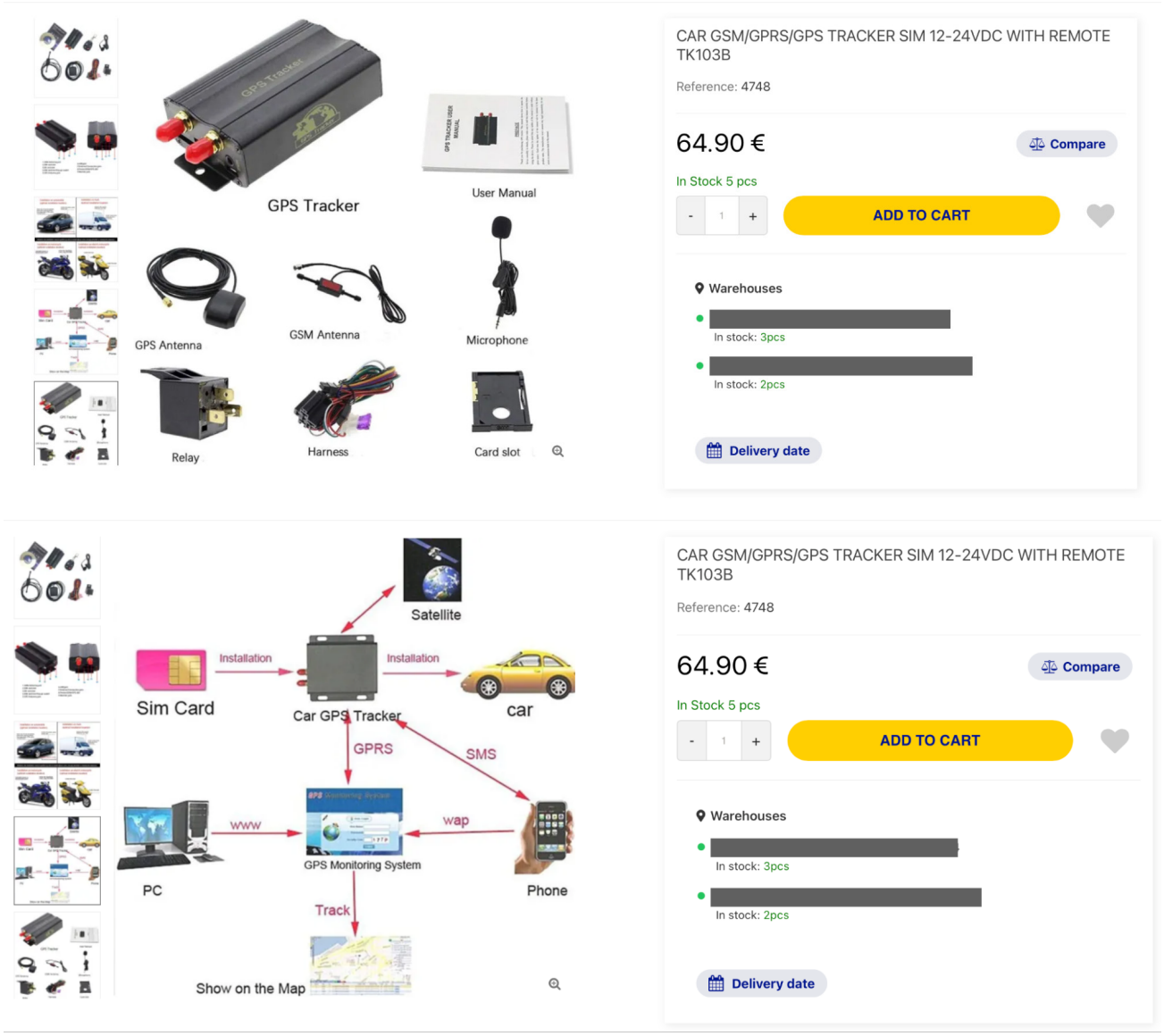
En un caso de 2023,no denunciado anteriormente, VEsinFiltro documentó un rastreador GPS escondido dentro de la cabina de un vehículo utilizado por familiares de un preso político.[83] El dispositivo es compatible con los



Imágenes del dispositivo dentro del vehículo de la víctima mientras estaba en proceso de ser desinstalado. Secciones de la imagen están pixeladas o desenfocadas para proteger su privacidad. (Fuente: VEsinFiltro)

modelos de rastreador GPS TK-103, que pueden conseguirse con varios fabricantes chinos. Este diseño de generación anterior requiere una tarjeta SIM para comunicaciones celulares GSM/GPRS, compatible con mensajes SMS, llamadas de voz y datos celulares de bajo ancho de banda.

La unidad estaba oculta tras cubiertas de plástico del tablero y conectada al sistema eléctrico del vehículo para poder mantenerse recargado. El dispositivo fue descubierto por un mecánico que llevaba a cabo un servicio de mantenimiento del vehículo y buscaba la causa de un problema eléctrico que se manifestó una semana después de que uno de los familiares fuese al centro penitenciario donde estaba la persona detenida. Durante la visita el vehículo permaneció fuera de la vista de sus propietarios durante al menos una hora; ese es el momento cuando podría haberse dado la instalación. Los problemas mecánicos que llevaron al descubrimiento sugieren que la instalación pudo haberse realizado apresuradamente o por



Listado de productos de un rastreador GPS TK103 similar que muestra los componentes clave y susoperación. (Fuente: ABCLED)[84]

personal sin experiencia técnica, lo que hizo que dañaran inadvertidamente los sistemas del vehículo. En general, los rastreadores ocultos en las cabinas de los vehículos son especialmente difíciles tanto de insta-

lar como de identificar. Los modelos observados funcionan con los sistemas eléctricos del vehículo, lo que permite un funcionamiento por tiempo indefinido sin necesidad de cambiar la batería.

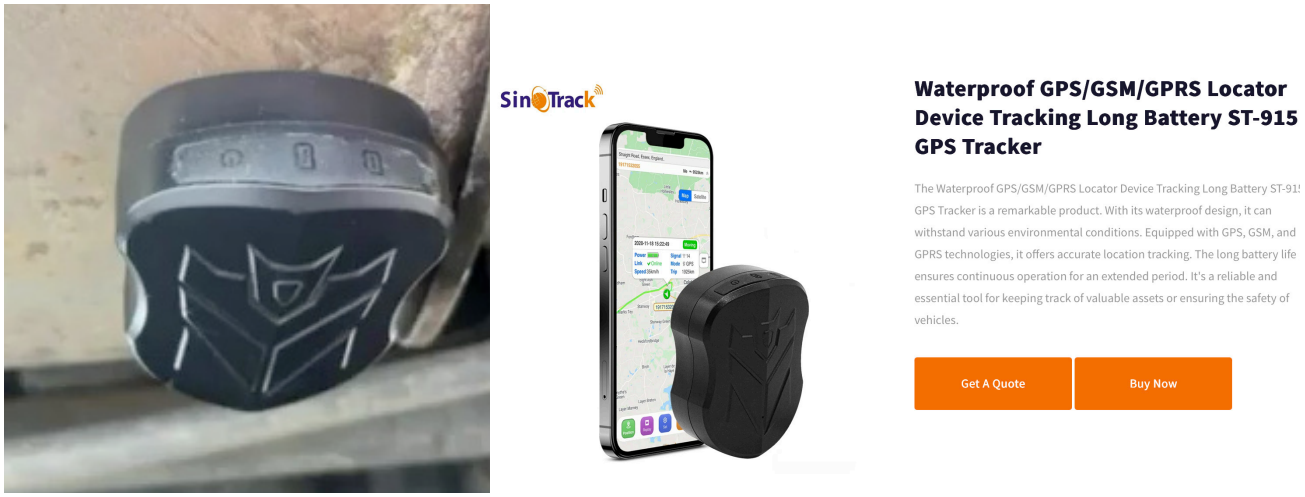
El micrófono integrado permite escuchar conversaciones del vehículo marcando el número de teléfono del rastreador cuando el modo de monitoreo está activado. Los operadores envían comandos a las unidades TK103 por SMS y llamadas al número de teléfono de la tarjeta SIM. Los usuarios pueden monitorear la ubicación del vehículo a través del sitio web del fabricante o directamente desde la unidad mediante mensajes SMS con coordenadas GPS y enlaces a mapas, ya sea a pedido o automáticamente a intervalos establecidos cuando el vehículo se mueve. Los portales en línea o las aplicaciones móviles permiten a los operadores revisar el historial de rutas y movimientos, configurar alertas de geofencing y acceder a funciones de monitoreo adicionales.

Rastreadores externos

Los rastreadores externos ofrecen una funcionalidad similar a la de los internos, pero resultan mucho más fáciles de instalar para las fuerzas de seguridad, pues los breves periodos en los que los vehículos están estacionados sin supervisión ofrecen tiempo suficientes para instalación. Funcionan con baterías internas en lugar de la energía del vehículo, mas estas baterías pueden durar varios meses, según el modelo y los patrones de uso. Cuando los dispositivos se acercan al límite de batería los operadores podrían, hipotéticamente, intercambiar unidades para mantener una vigilancia continua.

El 15 de septiembre de 2025 Margareth Baduel, activista en favor de los presos políticos, denunció públicamente a través de redes sociales la presencia de un dispositivo rastreador en uno de los vehículo de su familia.[85] El dispositivo fue identificado como un rastreador GPS. Margareth Baduel es hermana del preso político Josnars Baduel e hija del general Raúl Isaías Baduel, exministro de Chávez que murió en detención en 2021.[86]

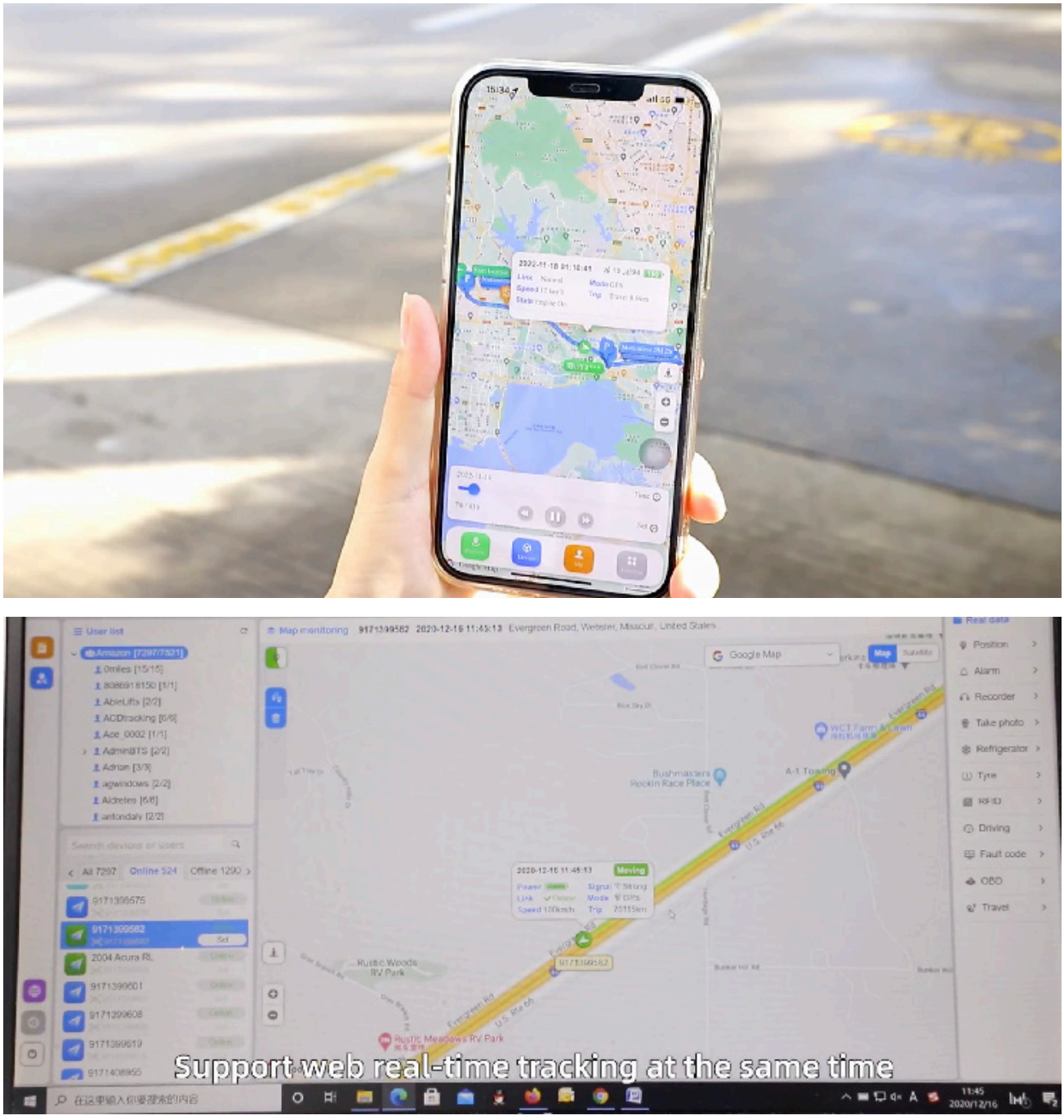
El rastreador en el carro de Baduel estaba fijado magnéticamente a la parte inferior trasera del vehículo, como se documenta en varios videos. Tras la difusión del hallazgo del rastreador en redes sociales, agentes de la División de Investigación Criminal de la Policía Nacional Bolivariana acudieron rápidamente al lugar para recuperar el dispositivo sin dar explicaciones.[87]



Izquierda: Extracto de un video publicado por el Comité por la Libertad de los Presos Políticos (CLIPPVE) que muestra el rastreador GPS instalado debajo del vehículo. Derecha: Captura de pantalla parcial del sitio web de SinoTrack.Fuentes: @clippve en X; SinoTrack)

La unidad coincide visualmente con el modelo SinoTrack 915L o con el modelo 915, que es ligeramente menos funcional. Los modelos SinoTrack 915L y 915 requieren tarjetas SIM operativas y aceptan comandos SMS. SinoTrack ofrece aplicaciones móviles e interfaces web para la monitorización y gestión de grandes cantidades de unidades, reproducción del historial de rutas y otras funciones diseñadas para aplicaciones de gestión de flotas, que las fuerzas de seguridad han reutilizado para la vigilancia política.

El dispositivo incluye un micrófono que puede capturar conversaciones del entorno, aunque su eficacia para grabar conversaciones dentro de vehículos probablemente se vea limitada por la ubicación del montaje, bajo el chasis. La ubicación óptima del micrófono para la vigilancia del interior del vehículo requeriría una instalación interna, lo que sugiere que la capacidad de audio de este rastreador externo podría servir



/Fotogramas de un video que muestra la función de reproducción de movimientos históricos registrados por un rastreador, además del seguimiento en tiempo real en el listado de Amazon del ST-915L. (Fuente: Sinto Track, Amazon.com)[88]

principalmente como inteligencia complementaria cuando los objetivos salen de los vehículos. La batería dura hasta 120 días en modo inactivo, que es el modo en el que los operadores solicitan la ubicación por SMS o llamadas. Los modos alternativos que permiten actualizaciones automáticas de ubicación a distintos intervalos ofrecen una duración de batería más corta, pero informes de posición más frecuentes. La batería dura varios meses y permite operaciones de vigilancia prolongadas sin necesidad de acceder de modo directo ni repetidamente a los vehículos que se busca rastrear.

Impactos en los derechos humanos de la vigilancia del movimiento

Vigilancia con drones por parte de las fuerzas de seguridad que operan dentro de un contexto en el que las libertades fundamentales están restringidas genera graves impactos en los derechos humanos. Además de la recopilación de datos de vigilancia, las fuerzas de seguridad emplean drones como armas psicológicas para suprimir la movilización de la oposición. La posibilidad de vigilancia aérea produce efectos intimidatorios y la sensación generalizada de vigilancia erosiona la organización comunitaria y las iniciativas de protesta a pequeña escala, incluso en ausencia de acciones directas de control. La función de intimidación opera mediante múltiples mecanismos. En primer lugar, la presencia visible de drones sobrevolando indica a los participantes de las protestas que las autoridades están monitoreando y grabando sus actividades. En segundo lugar, los funcionarios gubernamentales y los medios de comunicación estatales amplifican deliberadamente el mensaje de vigilancia mediante la difusión de imágenes de drones que muestran actividades de la oposición. En tercer lugar, en el contexto de la persecución documentada de quienes participan en protestas mediante detenciones arbitrarias, procesamientos y encarcelamientos, las personas se dan cuenta de que la vigilancia aérea crea registros de identificación que pueden usarse en su contra.

La ausencia de reglas y controles significativos que limiten el despliegue de la vigilancia, las políticas de retención de datos, las restricciones de acceso, los mecanismos de supervisión independientes y los recursos para las víctimas permite el abuso. Aunque las protestas ocurran en espacios públicos, la vigilancia aérea persistente, análoga a los sistemas de CCTV, captura detalles que afectan colectivamente la privacidad: quién asistió, con quién se asoció, cuánto tiempo estuvo y cuáles fueron sus patrones de movimiento. En contextos de persecución esta información se convierte en riesgo material que afecta la seguridad y las libertades personales. Al asistir a eventos políticos, las personas son objeto de vigilancia aérea que puede circular a través de canales progubernamentales o utilizarse como prueba para justificar ataques, un medio coercitivo para restringir el pleno ejercicio de los derechos políticos.

La legislación venezolana exige autorización judicial para las medidas de vigilancia intrusiva que impliquen la manipulación de vehículos o el acceso a espacios privados. En concreto, los dispositivos de escucha que graban conversaciones ambientales requieren que los fiscales obtemga autorización judicial para lo cual deben indicar claramente el delito investigado, los medios técnicos empleados, el lugar de despliegue y una duración no superior a treinta días.[89] En la práctica, los casos documentados de despliegue de rastreadores GPS no revelan supervisión judicial y los familiares afectados por estos dispositivos no han recibido notificación legal ni explicación alguna sobre su instalación. La naturaleza encubierta de la vigilancia GPS implica que muchos objetivos pueden ignorar que están bajo vigilancia durante largos períodos, durante los cuales las autoridades recopilan información exhaustiva sobre las redes, actividades y patrones operativos de la oposición.

El despliegue sistemático de tecnologías de vigilancia del movimiento, tanto aéreas como terrestres, sin supervisión judicial, restricciones legales ni transparencia, socava fundamentalmente la libertad de reunión y asociación garantizada por el derecho internacional de los derechos humanos. La Comisión Interamericana de Derechos Humanos ha reconocido que la vigilancia generalizada, que genera un temor razonable a la identificación y posterior persecución, impide efectivamente el ejercicio del derecho de reunión, incluso cuando no existen prohibiciones directas. La infraestructura de vigilancia de movimiento en Venezuela

Aplicaciones digitales patrocinadas y administradas por el Estado

Durante la última década se ha consolidado en Venezuela una red de vigilancia tecnológica de doble uso. En el discurso oficial, estas herramientas digitales se presentan como instrumentos para optimizar la prestación de servicios públicos. Sin embargo, la evidencia acumulada indica que esta infraestructura se ha utilizado principalmente para la recopilación sistemática y a gran escala de datos personales y para el control social.

El Estado venezolano ha impulsado una sistematización del uso de plataformas del control ciudadano mediante el despliegue de aplicaciones digitales. El Sistema Patria, presentado como una plataforma de protección social, y VenApp, promovida como una herramienta de servicio ciudadano, constituyen los dos pilares centrales del ecosistema de aplicaciones gubernamentales. Juntos, permiten la extracción sistemática de información, la clasificación de la población y la aplicación de mecanismos de control social. Su arquitectura sociotécnica revela cómo los regímenes autoritarios utilizan las plataformas digitales para transformar la prestación de asistencia social y el acceso a los servicios públicos en instrumentos de control político.

El Sistema Patria

La empresa china ZTE jugó un papel central en el desarrollo de la base de datos del Carnet de la Patria, incorporando capacidades avanzadas de identificación y recopilación masiva de datos.[90] El Sistema Patria y la Carnet de la Patria se han convertido en los principales canales de acceso a subsidios y programas de asistencia social, a la vez que sirven como instrumentos de presión económica y control de comportamiento. La dependencia de millones de personas a estos beneficios transforma el sistema en una herramienta que condiciona la subsistencia diaria al registro obligatorio y al suministro constante de información personal.

Un elemento particularmente revelador es que el dominio web de la plataforma (patria.org.ve) está registrado a nombre del Partido Socialista Unido de Venezuela (PSUV), en lugar de alguna agencia estatal.[91] Este hecho demuestra la fusión operativa entre el aparato estatal y la estructura partidaria y desdibuja cualquier separación funcional entre políticas públicas y control político, al tiempo que subordina los datos de millones de ciudadanos a una lógica de lealtad y utilidad partidaria.El acceso a las prestaciones sociales no es automático ni transparente; está condicionado al registro y al suministro continuo de información dentro del sistema, sin criterios transparentes de asignación. Para mantener la elegibilidad y aumentar las posibilidades de recibir beneficios sociales, los usuarios deben actualizar periódicamente sus datos y responder a encuestas sobre su situación socioeconómica y hábitos de consumo. En la práctica, este diseño convierte la necesidad de acceder a bienes esenciales y prestaciones sociales en un incentivo permanente para actualizar la información que el ciudadano proporciona al Estado.

El diseño técnico del sistema refuerza la lógica del control autoritario. Una parte significativa de la información recopilada por el Sistema Patria se centra en las relaciones de los usuarios con otras personas e instituciones, lo que permite a los administradores crear mapas detallados de las conexiones entre los ciudadanos, incluso si estos no utilizan la plataforma. Algunos ejemplos incluyen el registro de miembros del hogar y otros familiares directos, el registro de amigos y conocidos en la misión “Vuelta a la Patria” (para reportar el retorno de familiares migrantes que podrían no estar registrados), profesionales de la salud que han prestado servicios al usuario, registros de transferencias bancarias realizadas y recibidas, incluyendo datos personales de las contrapartes e identidades de las personas de contacto en organizaciones locales del Estado como los Consejos Comunales y las cadenas de distribución de alimentos (CLAP) además del registro de personas a quienes los usuarios prestan sus vehículos motorizados, entre otros.Es importante mencionar que la plataforma no ofrece ningún control ni verificación de autorización para el suministro de datos personales de terceros, ni políticas de gestión o protección de datos accesibles en la plataforma o en la Play Store de Google.

Otro aspecto destacable de la implementación de la plataforma del Sistema Patria es la limitación técnica del acceso de usuarios desde fuera de Venezuela. Para empezar, la aplicación móvil no está disponible en Google Play Store para dispositivos fuera del país. Además, el sistema utiliza técnicas de geoperimetraje (o geofencing), una técnica que impide el acceso a los servidores relevantes desde fuera del país. El sistema verifica el país reportado por la red para confirmar que se accede a la aplicación desde Venezuela. De lo contrario, se denegará el acceso.

Este control político tiene una de sus expresiones más visibles en el ámbito electoral a través de los llamados "puntos rojos", quioscos del PSUV instalados cerca de los colegios electorales los días de las elecciones. Aunque formalmente se presentan como espacios para fomentar la participación electoral y brindar orientación sobre el proceso, en la práctica funcionan como mecanismos para monitorear si los usuarios del Carnet de la Patria han votado. En estos puntos rojos el personal del partido gobernante registra la asistencia de los votantes escaneando el código QR en sus Carnets de la Patria o ingresando manualmente sus datos de identificación personal en una base de datos del partido. El partido gobernante usa esa información para llamar a los beneficiarios de asistencia social a votar si no se han presentado en los centros electorales a primera hora de la mañana. Después del día de las elecciones, quienes votaron pueden recibir un bono extra, mientras que a los que se abstuvieron se les pueden negar beneficios sociales. De esta manera, el acto de votar, que debería ser voluntario y libre de presiones, se integra en un sistema de recompensas y castigos mediados por plataformas digitales. Si bien los puntos rojos no permiten verificar el contenido del voto, cuando se estableció este mecanismo en 2018 se extendió una teoría conspiratoria que afirmaba que el código QR de alguna manera permitía verificar el contenido del voto.[92] Aunque esto no fuese técnicamente factible, algunas personas estaban convencidas y por ello se sintieron forzadas a votar por el partido gobernante.

Los puntos rojos encarnan así la convergencia entre vigilancia tecnológica y control político, reforzando la percepción de monitoreo constante y facilitando una coerción indirecta que afecta el ejercicio efectivo de los derechos políticos, especialmente entre las poblaciones más dependientes de la asistencia estatal.

VenApp

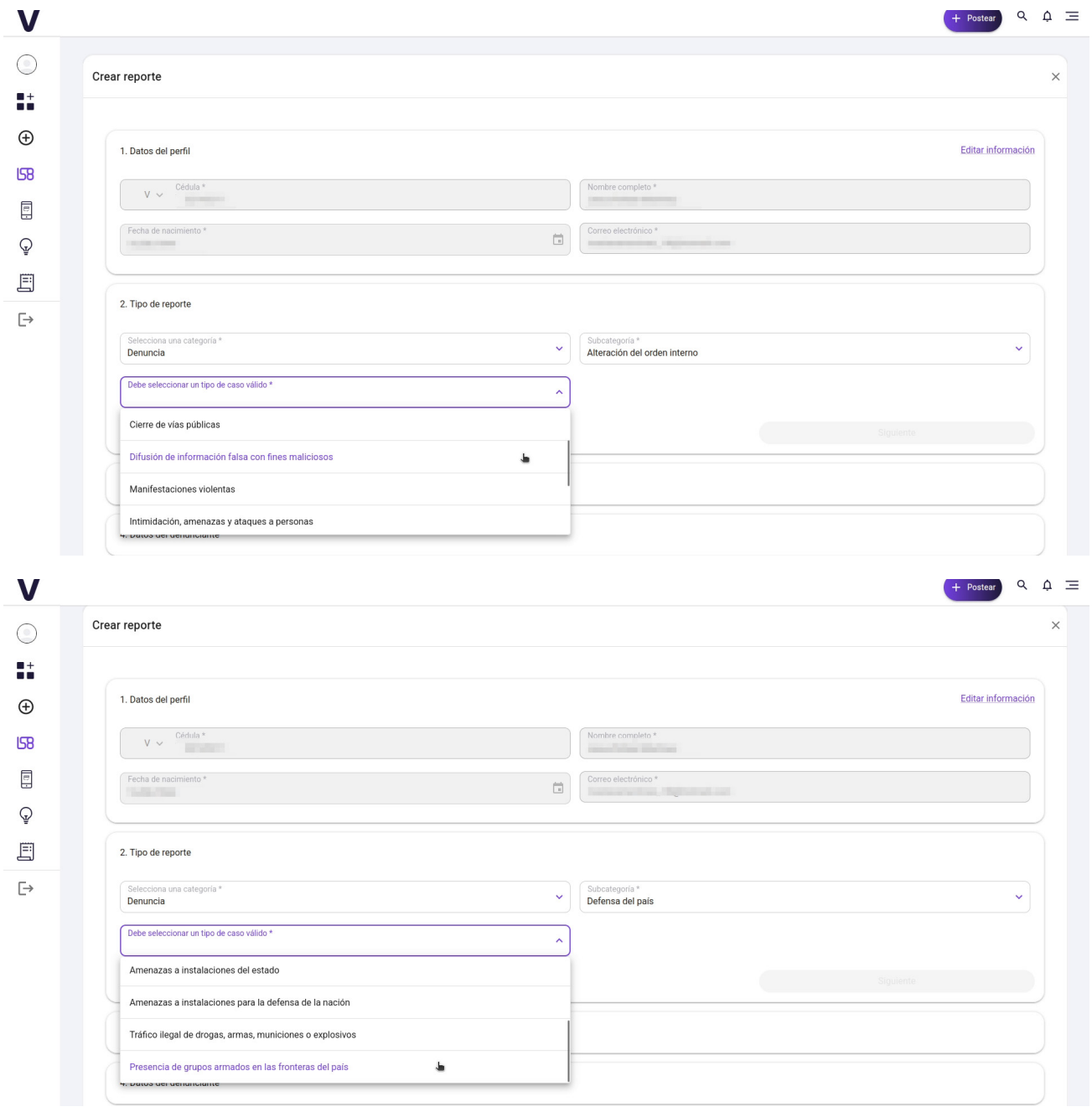
VenApp es una pieza más reciente en el ecosistema digital del régimen venezolano. A diferencia del Sistema Patria, cuyo enfoque central es el monitoreo coercitivo individual y económico, VenApp desplaza el foco hacia la vigilancia colectiva y promueve lo que puede describirse como una institucionalización de la denuncia vecinal. Esto bajo la apariencia de una super aplicación social que incluye una herramienta para informar problemas con servicios gubernamentales.

VenApp proporciona una plataforma tecnológica para denuncias que el chavismo intentó institucionalizar desde al menos 2008, cuando intentó aprobar la Ley de Inteligencia y Contrainteligencia, que obligaba a los ciudadanos a colaborar con los servicios de inteligencia proporcionando información sobre personas críticas al gobierno. Esta ley fue conocida popularmente como la "Ley Sapo", que es como la gente en Venezuela suelen llamar a los soplones. La indignación pública fue tan intensa que la ley fue derogada dos semanas después de su aprobación.[93]

Inicialmente, una versión precursora de VenApp fue diseñada para monitorear la movilización electoral de los simpatizantes del PSUV durante las elecciones a gobernadores de 2021. Posteriormente, en 2022, se abrió al público en general como una aplicación de mensajería venezolana con canales públicos similares a Telegram y un canal para compartir fotos similar a Instagram. La aplicación ganó fuerza en 2023 cuando se relanzó como una plataforma para informar fallas en servicios públicos, aprovechando su capacidad para compartir geolocalización.[94] Inmediatamente después de las elecciones presidenciales de julio de 2024, se agregó una nueva función a la aplicación para permitir denuncias de protestas y de participantes en la organización electoral de la oposición. [95]

VenApp se basa en una plataforma comercial desarrollado por una empresa con sede en Panamá que se adapta a diversos casos de uso para diferentes clientes.[96] Es por ello que una misma aplicación ha tenido diferentes funciones y casos de uso en tan solo cinco años. Técnicamente, VenApp tiene una estructura de

datos más estandarizada que el Sistema Patria, y por lo tanto, no solicita directamente información sensible como afiliación política o datos de identificación personal. Sin embargo, la función de generación de informes presenta un problema importante. La interfaz de la aplicación ofrece categorías de reporte que históricamente se han asociado con la persecución política y los criterios para clasificar eventos bajo estas categorías pueden aplicarse arbitrariamente. Este es el caso de categorías como “Presencia de personas sospechosas en el territorio nacional”, “Avistamientos de drones”, “Alteración del orden público”, “Cierre de vías públicas”, “Difusión de información falsa con fines maliciosos” e “Intimidación, amenazas y ataques contra personas”. Otra característica que representa un riesgo directo es la constante solicitud de la aplicación a los usuarios para que compartan su geolocalización.



Interfaz de reportes de VenApp. (Fuente: VenApp)

Actualmente la función de delación canaliza estos reportes a la Fuerza Armada Nacional Bolivariana (FANB), las Unidades de Milicias Comunales y las Bases Populares de Defensa Integral.[97] Estas entidades reciben, procesan y eventualmente dan curso a las denuncias ciudadanas presentadas a través de la aplicación, en el marco del llamado Sistema de Defensa Territorial que, según el discurso oficial, tiene como objetivo fortalecer "la defensa del pueblo." [98]Esta formulación transformó lo que originalmente se comercializó como un canal de gobierno electrónico en un mecanismo que fomentaba la vigilancia entre pares, permitía informes geolocalizados de comportamiento políticamente indeseable y normalizaba la delación como un deber cívico.

Además de la información capturada explícitamente por el formulario de denuncia, la plataforma de VenApp incluye rastreadores y publicidad integrada en su código con identificadores asociados a Google AdSense y Facebook. Esto permite no solo que los administradores del sitio web moneticen el tráfico generado por los ciudadanos que utilizan la plataforma, sino también que se elaboren perfiles de usuario según sus hábitos de navegación. Esta información puede utilizarse para personalizar la publicidad y, potencialmente, para determinar las actividades específicas de cada usuario.

VenApp estuvo disponible originalmente en las tiendas de aplicaciones. Sin embargo, fue eliminada tanto de Google Play Store para dispositivos Android como de App Store para dispositivos iOS después de agosto de 2024, cuando el régimen venezolano empezó a promover abiertamente la aplicación como un canal para doxear a manifestantes y simpatizantes de la oposición. Las tiendas de aplicaciones no anunciaron oficialmente que fuera ese el motivo de la eliminación, pero el momento en el que lo hicieron lo sugiere. Desde entonces, VenApp se ha centrado en funcionar como una aplicación web, con menos esfuerzos para promover la instalación manual de la aplicación.

Instalar manualmente la aplicación en dispositivos Android fuera de la tienda de aplicaciones (o app store) expone a los usuarios a riesgos adicionales. El procedimiento, conocido como sideloading, se considera inseguro para los usuarios porque implica instalar software sin los niveles habituales de verificación, comprobaciones de integridad y actualizaciones que ofrecen las tiendas de aplicaciones oficiales. El sideloading hace a los usuarios más vulnerables a riesgos como la instalación de versiones alteradas de la aplicación con código malicioso y que puede facilitar el acceso no autorizado a datos personales. También es posible descargar una versión oficial del sistema operativo como vector para monitorear o recolectar información sensible, todo sin las salvaguardas que ofrecen la app store.

La lógica que subyace al diseño y uso de VenApp no surge de manera aislada, sino que se alinea con la doctrina comunicacional y organizacional expresada en documentos oficiales como el manual "Redes, calles, medios, muros y radio bemba."[99] En este texto el espacio digital se concibe como un frente permanente de acción política donde la vigilancia, el monitoreo ciudadano y la denuncia de conductas consideradas desviadas o amenazantes forman parte de la "batalla comunicacional". Esta doctrina legitima la participación activa de las estructuras civiles y comunitarias en las tareas de observación y denuncia, normalizando el uso de las plataformas digitales como canales institucionales para la recopilación de información ciudadana con fines de control político.

Ecosistema de aplicaciones

El Sistema Patria y VenApp no operan de forma aislada. Ambas plataformas contribuyen a una infraestructura de recopilación de datos más amplia para construir perfiles poblacionales integrales. Este proceso se desarrolla sin consentimiento informado y mediante mecanismos de interoperabilidad opacos entre diferentes instituciones estatales. A través del Sistema Patria, el Estado recopila una cantidad significativa de información confidencial, incluidos datos demográficos y socioeconómicos, registros de salud, transacciones bancarias y de criptomonedas, registros de beneficios estatales y afiliaciones a programas patrocinados por el gobierno.[100] El Sistema Patria interopera con los registros del Instituto Nacional de Transporte y del Instituto Venezolano de los Seguros Sociales, lo que permite la vinculación, verificación y actualización automática de los datos ciudadanos. La potencia del sistema reside no solo en el volumen de información que agrega, sino también en su capacidad de integración, que permite la construcción de perfiles individuales o poblacionales.

La violación de derechos fundamentales del Sistema Patria radica en condicionar el acceso a bienes y servicios esenciales a la provisión de datos para un sistema de vigilancia poblacional. En un contexto donde la hiperinflación y el colapso económico han destruido el poder adquisitivo y en el que aproximadamente el 80% de la población vive por debajo del umbral de pobreza, la distribución de alimentos y los subsidios estatales otorgan al partido gobernante un poder significativo sobre la población. Al condicionar el acceso a estos recursos al registro en un sistema que recopila una gran cantidad de datos personales, monitorea el comportamiento político y rastrea las relaciones sociales, el Estado transforma las necesidades básicas en un mecanismo de control político. Como principales cuidadoras en los hogares venezolanos, las mujeres tienen una responsabilidad desproporcionada en el acceso a los alimentos a través de los programas CLAP, la gestión de las finanzas del hogar y el mantenimiento de la elegibilidad familiar para recibir prestaciones sociales.

La ausencia de una legislación integral sobre protección de datos, sumada a la integración de tecnologías de rastreo e identificadores publicitarios en las aplicaciones estatales, propicia la explotación sistemática de los datos de los ciudadanos sin su consentimiento expreso ni posibilidad de recurso alguno. Tanto Patria como VenApp recopilan información exhaustiva sobre los usuarios y sus redes sociales, a la vez que incorporan tecnologías de rastreo comercial que perfilan a los usuarios con fines publicitarios. Los ciudadanos obligados a usar estas plataformas carecen de la capacidad práctica para rechazar el rastreo, no tienen acceso a información sobre cómo se utilizan o comparten sus datos, ni mecanismos legales para exigir responsabilidades o rectificación.

Otras aplicaciones digitales estatales vinculadas al ecosistema Patria incluyen criptomonedas y transferencias de dinero, pagos en puntos de venta, pagos subsidiados en gasolineras, suscripciones a beneficios en efectivo y programas de alimentos subsidiados:

vePatria

Incluye funciones para gestionar los beneficios más usados del Sistema Patria y con solicitudes afiliadas de recopilación de datos. Al momento de la publicación de este informe, esta aplicación móvil solo es accesible dentro de Venezuela y no está disponible en las tiendas de aplicaciones (app stores) oficiales.

veQR

Permite registrar el Carnet de la Patria, solicitar ayudas discrecionales en efectivo y registrarse para comprar alimentos subsidiados distribuidos por el programa CLAP. También se ha utilizado para facilitar el registro de participantes en mítines del partido gobernante.

veMonedero

Se enfoca en operaciones financieras como transferencias bancarias y otras transacciones, incluyendo recargas de teléfono y transacciones con criptomonedas. Esta aplicación permite enviar fondos a familiares y amigos y convertir criptomonedas a la moneda nacional.

vePDV

Se concentra en información y transacciones relacionadas con combustible. Además de mostrar las cuotas de combustible disponibles a precios subsidiados, incluye una lista y un mapa de estaciones de servicio cercanas al usuario junto con sus precios y disponibilidades. También permite el pago de recargas de combustible a través de billeteras registradas en el Sistema Patria.

Ciberpatrullaje y vigilancia de las redes sociales

La persecución de la expresión crítica en Venezuela se basa en un aparato de monitoreo digital progresivamente institucionalizado que incluye la vigilancia en plataformas abiertas. Esta práctica se intensificó tras la creación en 2013 del Centro Estratégico para la Seguridad y Protección de la Patria (CESPPA) que promovió la capacitación de las fuerzas de seguridad, incluyendo la Guardia Nacional Bolivariana, a utilizar las redes sociales como sistemas de alerta temprana contra expresiones consideradas disruptivas o contrarias al orden político.[101]

El monitoreo opera a través de ciberpatrullaje sistemático en plataformas de redes sociales, incluyendo X, Instagram, TikTok y Facebook, así como espacios de mensajería privada como WhatsApp y Telegram. Publicaciones, comentarios, hashtags y patrones de interacción son rastreados por agencias de inteligencia, particularmente el Servicio Bolivariano de Inteligencia Nacional (SEBIN), y utilizados como evidencia en investigaciones criminales. Este monitoreo se extiende más allá de figuras públicas o líderes políticos a ciudadanos comunes, periodistas, activistas y líderes comunitarios, abarcando la identificación de cuentas críticas al gobierno, el monitoreo de historiales de contenido y la vigilancia de mensajes distribuidos en espacios percibidos como privados o semiprivados, como grupos de WhatsApp. El monitoreo se complementa con el rol de individuos que, voluntariamente o bajo coerción, aceptan servir como informantes en las actividades de redes sociales y WhatsApp de sus vecinos y compañeros de trabajo.

Tras las elecciones presidenciales de julio de 2024 este tipo de monitoreo parece haberse intensificado significativamente, combinando campañas de intimidación, detenciones y el uso estratégico de plataformas digitales como herramientas de vigilancia y disuasión.[102] Durante este período el espacio digital se convirtió en una extensión directa del aparato de persecución estatal, con VenApp y Telegram cumpliendo un papel en la recopilación, sistematización y circulación de información personal sobre individuos identificados como partidarios de la oposición o testigos electorales.[103]

Esta sección examina los mecanismos y prácticas de ciberpatrullaje empleados por las fuerzas de seguridad venezolanas, las campañas sistemáticas de doxeo y acoso contra disidentes vinculados a la "Operación Tun Tun" (llamada así por el sonido de los golpes en las puertas) los patrones evidentes en los arrestos y procesamientos por expresión en Internet y los impactos resultantes en la libertad de expresión y de reunión.

4.1. Ciberpatrullaje y doxeo: la maquinaria de la persecución digital

Las fuerzas de seguridad venezolanas llevan a cabo un ciberpatrullaje sistemático en redes sociales y aplicaciones de mensajería para identificar, rastrear y recopilar información sobre personas que se expresan en línea criticando al gobierno. Esta vigilancia opera a través de múltiples canales institucionales, siendo el SEBIN y la Dirección General de Contrainteligencia Militar (DGCIM) las principales agencias de inteligencia, con el apoyo de las fuerzas policiales regionales y municipales que hacen un monitoreo localizado. Como complemento a estas operaciones oficiales, redes coordinadas de cuentas, troles y presuntos bots amplifican simultáneamente las narrativas progubernamentales y hostigan a los disidentes.

Estas redes operan con aparente coordinación entre plataformas, particularmente en Telegram, donde canales como "Caza Guarimbas VE" compilaron y difundieron sistemáticamente listas de doxeo que contenían nombres, fotografías, direcciones, números de identificación y otra información personal de individuos identificados como partidarios de la oposición, manifestantes u observadores electorales.[104] La información recopilada facilita posteriores detenciones, acoso y represalias contra personas identificadas y sus familias. Esta práctica se intensificó drásticamente tras las elecciones de julio de 2024, cuando los canales de Telegram se convirtieron en repositorios centrales de datos personales utilizados como arma contra personas acusadas de ser disidentes.

La “Operación Tun Tun” se relanzó el 29 de julio de 2024 como una campaña de arrestos puerta a puerta tras los controvertidos resultados de las elecciones presidenciales.[105] La operación integró múltiples flujos de vigilancia en un mecanismo de persecución coordinado, que incluía informes y doxeo a través de VenApp y grupos de Telegram. La operación funcionó como una forma de persecución física y de guerra psicológica. Las fuerzas de seguridad publicaron más de 65 piezas audiovisuales asociadas a la “Operación Tun Tun”, la mayoría de las cuales presentaban una tipografía idéntica y el lema “Sin lloradera”.[106]tos materiales exhibieron dos patrones principales: videos que mostraban a manifestantes en protestas, seguidos de imágenes de su captura y confesiones forzadas, generalmente presentados con tonos de burla, efectos de sonido y animaciones de rejas de prisión cerrándose. También se circularon videos que retomaban estéticas de películas de terror, incluida música de películas como Child’s Play y Saw, acompañado de mensajes amenazantes y referencias a personajes de terror como Chucky y Jigsaw para maximizar el impacto psicológico.

El contenido se originó principalmente del programa de televisión de Diosdado Cabello Con el mazo dando y sus cuentas de redes sociales asociadas en Telegram e Instagram fueron posteriormente republicadas por otros usuarios y adoptadas por las cuentas oficiales de las fuerzas de seguridad, incluida la Policía Nacional Bolivariana (PNB), la DGCIM y las fuerzas policiales regionales y municipales. VEsinFiltro documentó al menos 55 casos de arresto entre julio de 2024 y enero de 2025 en los que las fuerzas de seguridad utilizaron a personas detenidas para propaganda en redes sociales, con 27 explícitamente vinculadas a la “Operación Tun Tun” mediante el uso de sus elementos audiovisuales característicos o menciones en etiquetas y descripciones.[107]

Muchos videos captaron patrullas llegando a las casas de las personas, con agentes armados y encapuchados llevándolas detenidas a la comisaría. Grabaciones en primer plano obligaron a los detenidos no solo a confesar presuntos delitos (generalmente “incitación al odio” o “terrorismo”), sino también a disculparse con el gobierno e incriminar a líderes políticos democráticos. Entre los casos documentados se encuentra el de María Oropeza, coordinadora del partido político Vente Venezuela en el estado Portuguesa, quien transmitió en vivo un video de su arresto el 7 de agosto de 2024, en el que se vio a agentes de la DGCIM irrumpiendo en su domicilio con palancas de hierro y sin orden judicial.[108] La exhibición pública de arrestos, “confesiones” forzadas y acusaciones severas refuerza la lógica intimidatoria y promueve la autocensura entre la población.[109]

Patrones de persecución penal por la expresión en Internet

Desde 2020 se ha observado una notable tendencia a la persecución penal de periodistas y ciudadanos comunes como consecuencia directa de las expresiones personales compartidas en entornos digitales. Estos casos revelan patrones consistentes de cómo el régimen venezolano utiliza la vigilancia digital como arma contra la libertad de expresión. El análisis de los casos documentados revela varios patrones recurrentes.

En primer lugar, las investigaciones se originan a partir de la vigilancia digital sistemática en lugar de los procedimientos de investigación tradicionales. En estos procesos el ciberpatrullaje sirve tanto como catalizador de las investigaciones criminales como su principal base probatoria. Los fiscales se basan en gran medida en contenido digital descontextualizado (publicaciones, mensajes, imágenes y videos) reinterpretado desde una perspectiva criminal, sin análisis contextual ni evidencia de daño concreto o una relación causal directa con hechos materiales verificables. La valoración probatoria se basa principalmente en declaraciones de oficiales de agentes de la policía que participaron en el ciberpatrullaje y la revisión de contenido digital. Esta valoración carece de informes técnicos especializados, o de análisis forense independiente para establecer de manera concluyente la autoría o procedimientos adecuados de cadena de custodia para la evidencia digital. El caso de Juan Francisco Alvarado, estudiante de periodismo detenido el 20 de marzo de 2025 y posteriormente sentenciado a 15 años de prisión por presunta incitación al odio ejemplifican este uso del ciberpatrullaje como herramienta para criminalizar la expresión en línea. Según los registros judiciales, la investigación penal se centró en un monitoreo amplio y prolongado de su actividad digital en múltiples plataformas, sin una definición clara de criterios técnicos, plazo ni fundamento jurídico específico.[110]

En segundo lugar, las autoridades aplican disposiciones penales vagas y expansivas —en particular, la "incitación al odio" en virtud de la Ley Contra el Odio, para la Convivencia Pacífica y la Tolerancia, junto con los cargos de terrorismo, traición, conspiración y atentados contra el honor y la reputación— sin criterios claros de proporcionalidad, daño real o intencionalidad. Esto permite la criminalización de opiniones, denuncias ciudadanas o valoraciones políticas que constituyen un debate público legítimo. Las mujeres enfrentan vulnerabilidades particulares en este sistema: Marggie Orozco, una médico de 65 años de edad recibió 35 años de prisión por difundir un audio de WhatsApp criticando la gestión gubernamental y llamando a la participación electoral. Esto tras denuncia de miembros del consejo comunal que previamente la habían sometido a hostigamiento y amenazado con excluirla de beneficios sociales.[111] De igual manera, Randal Glendysmar Telles Peña, una mujer de 22 años fue condenada a 15 años por publicar un video crítico en TikTok. Los agentes de la DGCIM la localizaron y arrestaron en su lugar de trabajo. [112]

En tercer lugar, la vigilancia se extiende a espacios de comunicación semiprivados, con mecanismos de denuncia comunitarios que transforman a los vecinos en informantes. Múltiples casos documentados involucran arrestos derivados de mensajes grupales de WhatsApp o notas de voz compartidas en contextos comunitarios, incluyendo el de Marcos José Palma Martínez, condenado a 15 años por distribuir un audio crítico en un grupo comunitario de WhatsApp.[113]

En cuarto lugar, el personal militar enfrenta una vulnerabilidad particular: Jesús Gabriel Molina Sifontes, un oficial activo de la Fuerza Armada Nacional Bolivariana, recibió una sentencia de ocho años por desobediencia e incitación a la rebelión después de publicar un estado de WhatsApp en el que aparecía la bandera de Venezuela con siete estrellas.[114] La imagen fue reportada por un superior a la DGCIM pese a ausencia de elementos delictivos.[115]

En quinto lugar, las detenciones suelen ocurrir sin órdenes judiciales, precedidas de amenazas y acompañadas de largos periodos de incomunicación y denegación de representación legal. Los centros de detención incluyen la sede del SEBIN, las instalaciones de la DGCIM y las comandancias de la Guardia Nacional Bolivariana, todas con visitas severamente restringidas. El periodista Rory Branker, editor del medio digital La Patilla, fue detenido el 20 de febrero de 2025 tras compartir una imagen relacionada con las recompensas ofrecidas por el gobierno estadounidense contra altos funcionarios venezolanos.[116] Branker fue liberado el 4 de febrero de 2026, después de sufrir traslados arbitrarios y una prolongada desaparición forzada.

En sexto lugar, las violaciones procesales permean los procesos judiciales: la ausencia de pericia técnica independiente, la falta de protocolos forenses para validar la autenticidad de las pruebas digitales, la denegación de una defensa adecuada, la aplicación de la jurisdicción militar a civiles y la imposición de penas desproporcionadas e inconexas con la gravedad del presunto delito. El informe de octubre de 2024 de la Misión Internacional Independiente de Determinación de los Hechos de las Naciones Unidas sobre Venezuela documentó el caso de Whilfer Piña Azuaje, activista político detenido tras presuntamente publicar una amenaza contra el entonces presidente Maduro en un estado de WhatsApp. Las autoridades anunciaron la incautación y extracción de su teléfono móvil, con cargos que incluyen conspiración, asociación ilícita e intento de asesinato, únicamente sobre la base de un mensaje en redes sociales.[117]

Finalmente, la difusión pública de arrestos mediante videos de propaganda sirve como ejemplo y disuasión. Las fuerzas de seguridad difunden imágenes de detenciones, confesiones forzadas y cargos penales graves para reforzar la idea de que el Estado observa, identifica y castiga la disidencia incluso en sus formas más cotidianas.

Impactos en la libertad de expresión y de asociación

La convergencia de la vigilancia digital, el procesamiento selectivo y la detención arbitraria ha generado profundos impactos en la libertad de expresión en Venezuela. Estos efectos no constituyen episodios aislados de censura, sino un entorno comunicacional marcado por el miedo, la autocontención y una progresiva reducción del espacio cívico.

Una de las consecuencias más generalizadas es la normalización de la autocensura. La posibilidad real de que una publicación, audio o mensaje —incluso difundido en espacios cerrados o comunitarios— pueda resultar en procesos penales, detención o represalias ha llevado a amplios sectores de la ciudadanía a moderar su lenguaje, evitar temas delicados o abstenerse por completo de opinar sobre asuntos de interés público. Este silenciamiento preventivo se produce en un contexto de inseguridad jurídica, donde no existen criterios claros sobre qué tipo de expresión puede considerarse delictiva. La aplicación discrecional de disposiciones penales amplias refuerza la percepción de riesgo permanente y transforma la expresión digital en una actividad potencialmente peligrosa.

Para periodistas y activistas, los mecanismos descritos han provocado desplazamientos forzados, tanto internos como transnacionales. Temor a la detención arbitraria, encarcelamiento prolongado en condiciones severas y persecución familiar obligó a cientos de personas a abandonar sus comunidades, empleos y redes sociales. Este desplazamiento forzado no solo afecta a las personas, sino que también debilita la capacidad organizativa de la sociedad civil.

Los mecanismos de denuncia comunitaria y las denuncias inducidas generan efectos disuasorios adicionales sobre la cohesión social y la acción colectiva. La posibilidad de una denuncia por parte de un vecino, miembro del consejo comunitario o conocido transforma la interacción social en un terreno de sospecha, debilitando la cohesión comunitaria y la acción colectiva.

Las detenciones, condenas y procesos penales por expresiones digitales cumplen además funciones ejemplarizantes y disciplinarias. La difusión pública de arrestos, acusaciones graves o “confesiones” grabadas refuerza la idea de que el Estado observa, identifica y castiga la disidencia incluso en sus formas más cotidianas. Este efecto no requiere una persecución masiva para ser efectivo: los casos visibles con sanciones desproporcionadas producen un impacto inhibitorio generalizado.

Intercepción de telecomunicaciones privadas

La intercepción privada de telecomunicaciones representa uno de los componentes más intrusivos del aparato de vigilancia de Venezuela, violando directamente las comunicaciones privadas de millones de ciudadanos mediante prácticas sistemáticas y generalizadas que superan con creces cualquier justificación legítima de las fuerzas del orden. El marco constitucional y legal venezolano protege nominalmente la privacidad de las comunicaciones mediante múltiples disposiciones superpuestas. El artículo 60 de la Constitución de la República Bolivariana de Venezuela (CRBV) garantiza a toda persona el derecho a la protección de su vida privada y el derecho a acceder a la información personal recopilada por el Estado, al tiempo que exige que la recopilación de datos respete la privacidad.[118] La Ley Orgánica de Telecomunicaciones (2000) establece que las solicitudes de intercepción de telecomunicaciones sólo pueden realizarse después de que los fiscales obtengan la aprobación del tribunal en el marco de una investigación criminal.[119] La Ley de Protección de la Privacidad de las Comunicaciones de 1991 estipula que las comunicaciones privadas solo pueden ser interceptadas por orden judicial en circunstancias limitadas, incluidos los delitos contra la seguridad del Estado, el patrimonio público, los narcóticos, el secuestro y la extorsión. S[120]in embargo, la enorme disparidad entre las protecciones legales y la práctica documentada revela una indiferencia sistemática por las limitaciones legales y las normas internacionales de derechos humanos.

A diferencia de otros métodos de vigilancia, como las cámaras CCTV o el monitoreo con drones, la intercepción de telecomunicaciones no suele dejar evidencia que las personas afectadas puedan detectar o documentar. Comprender la escala y la naturaleza de estas prácticas requiere distinguir entre la intercepción de contenido (la sustancia real de las comunicaciones, incluyendo el audio de las llamadas, mensajes de texto y el tráfico de Internet) y la recopilación de metadatos (información sobre las comunicaciones, incluidos números de teléfono, marcas de tiempo, duración y datos de ubicación). Las violaciones de la privacidad y las capacidades de vigilancia difieren sustancialmente entre estas categorías.

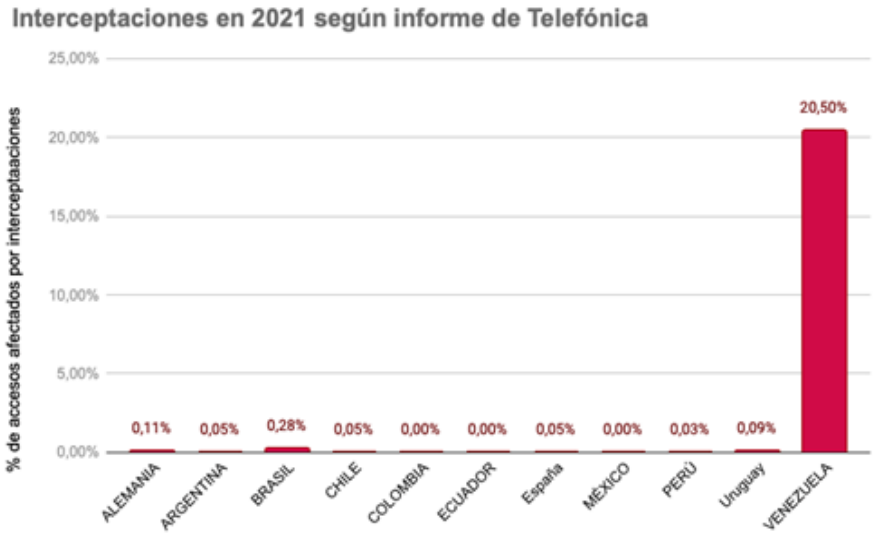
Las siguientes secciones analizan la intercepción de telecomunicaciones a escala masiva, la migración de poblaciones vulnerables a aplicaciones de mensajería cifrada que reducen la efectividad de la intercepción tradicional, las capacidades de vigilancia del tráfico de Internet que han sido desplegadas por el proveedor de telecomunicaciones estatal CANTV, el seguimiento de la ubicación mediante la cooperación del proveedor y dispositivos receptores IMSI no autorizados, y los impactos de esta vigilancia generalizada en los derechos humanos de la sociedad civil venezolana.

Intercepción de telecomunicaciones privadas a gran escala

Desde 2011 las llamadas telefónicas privadas de periodistas y representantes políticos se graban sistemáticamente y luego se transmiten en los medios estatales, a menudo editadas o manipuladas con fines incriminatorios, lo que demuestra una indiferencia sistemática por las protecciones legales.[121] Los venezolanos han estado reportando "llamadas interceptadas" y mensajes SMS por años, desde 2007. Sin embargo, estos relatos seguían siendo en gran medida anecdóticos, difíciles de verificar sistemáticamente. Un avance crucial se produjo en 2021, cuando la compañía española Telefónica, la matriz de Movistar Venezuela, publicó datos cuantitativos en su informe de transparencia. El informe reveló que durante 2021 Movistar facilitó la intercepción de contenido de comunicaciones de más de 1,5 millones de líneas de abonados, aproximadamente el 21% de la base total de clientes de Movistar Venezuela.[122]La divulgación de datos de Telefónica abarca llamadas, mensajes, ubicación celular y tráfico de Internet sin desagregar los diferentes tipos de intercepción.

Esta tasa de intercepción es alarmantemente desproporcionada y difícil de conciliar con un uso estrictamente excepcional, individualizado y proporcional en investigaciones penales. En otros mercados de Telefónica en Latinoamérica y Europa el porcentaje de líneas interceptadas no alcanzó el 1% de suscriptores. La tasa de intercepción de Venezuela superó así la de mercados comparables más de veinte veces, lo que indica un abuso sistémico más que una actividad policial específica. La escala demuestra una inversión gubernamental sustancial en el procesamiento de volúmenes masivos de datos recopilados por este aparato de vigilancia.

Cuota de líneas de abonado de Telefónica y sus filiales afectadas por intercepciones de telecomunicaciones en 2021 por mercado, según datos publicados por Telefónica. (Fuente: VEsinFiltro)[123]



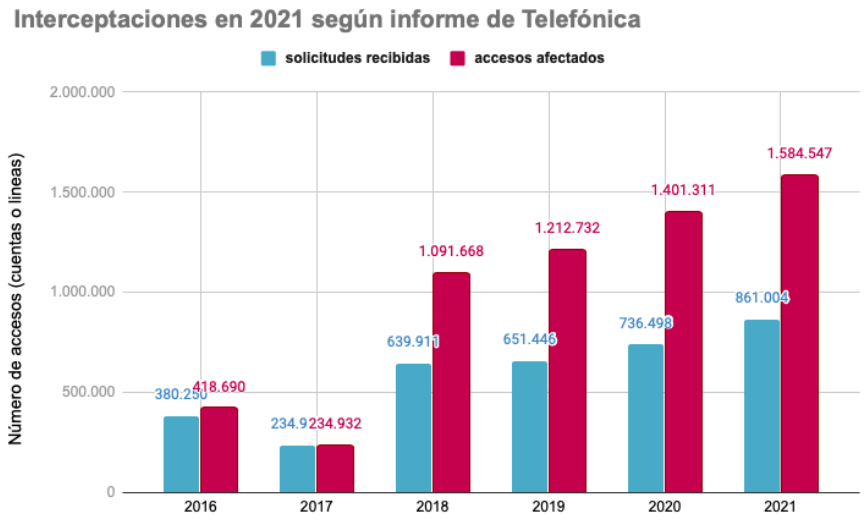
La progresión de las intercepciones a lo largo del tiempo revela la creciente vigilancia gubernamental. El número de líneas de abonados afectadas por intercepciones se multiplicó por siete entre 2016 y 2021, pasando de 234.932 líneas a 1.584.547.[125] Esta importante expansión ocurrió durante un período de intensificación de la represión política tras las victorias electorales de la oposición en 2015 y la aceleración a través de la crisis constitucional de 2017 y el malestar popular, lo que sugiere una correlación entre la expansión de la vigilancia y la consolidación autoritaria.[126]

Los datos sobre órdenes de intercepción gubernamentales desaparecieron de los informes de transparencia de Telefónica posteriores a la publicación de 2021, lo que impidió el seguimiento público continuo de este abuso. Sin embargo, el informe de 2021 proporciona una ventana crítica a prácticas que casi con certeza continúan en otros operadores de telecomunicaciones venezolanos que nunca han publicado datos de transparencia comparables.

Movistar también entregó metadatos del 13 por ciento de sus suscriptores durante 2021, brindando a las autoridades información sobre patrones de comunicación, redes de contacto, información del subscriptor y el historial de ubicación, incluso cuando no se interceptó el contenido de la comunicación.[127] Esta vigilancia de metadatos puede permitir el análisis de redes sociales, la identificación de estructuras organizativas y el seguimiento de movimientos individuales, capacidades especialmente valiosas para la vigilancia política dirigida a organizaciones de la sociedad civil, movimientos de oposición y periodistas independientes. El impacto acumulativo de la intercepción de contenido y metadatos afectó aproximadamente a un tercio de la base de suscriptores de Movistar, lo que crea una vigilancia generalizada que altera fundamentalmente cómo se comunican los venezolanos.

Los datos interceptados se hicieron accesibles a una lista extraordinariamente amplia y mal definida de “autoridades competentes” que contradicen tanto las garantías legales venezolanas como los estándares internacionales de derechos humanos. El informe de transparencia de Movistar Venezuela especificó que las solicitudes de intercepción no requerían órdenes judiciales, sino que podían ser presentadas por el Ministerio Público (Fiscalía General de la República), el CICPC (el principal organismo de investigación criminal de Venezuela), el Servicio Bolivariano de Inteligencia Nacional (SEBIN), las fuerzas policiales habilitadas para llevar a cabo investigaciones criminales, componentes de la Fuerza Armada Nacional Bolivariana, las autoridades de inteligencia policial, la Policía Nacional Bolivariana, cualquier otra entidad auxiliar de investigación criminal u otras entidades especiales de investigación penal e, inexplicablemente, la Universidad Nacional de Seguridad (UNES).[128]

Número de solicitudes de intercepción y número de líneas de subscriptores afectadas por intercepciones de telecomunicaciones por año, según datos publicados por Telefónica. (Fuente: VEsinFiltro)[124]



Esta amplia estructura de autorización creó las condiciones propicias para la intercepción indiscriminada y el abuso por parte de autoridades que operan al margen de la legislación venezolana y los estándares internacionales. La inclusión de instituciones universitarias de formación en seguridad entre las entidades autorizadas para solicitar la intercepción de telecomunicaciones pone en relieve la ausencia de una supervisión significativa o una evaluación de proporcionalidad. En un contexto de persecución política documentada, este acceso incontrolado a las comunicaciones privadas facilita violaciones sistemáticas de los derechos humanos.[129]

Es probable que los proveedores estatales de telecomunicaciones faciliten la vigilancia a tasas comparables o superiores a las de Movistar. CANTV, que opera como el principal proveedor de servicios de Internet residencial y es un importante operador de telefonía móvil (Movilnet), no está sujeto a supervisión independiente y se encuentra bajo control gubernamental directo. Los registros telefónicos permanecen accesibles a los fiscales sin autorización judicial.

Migración a aplicaciones de mensajería

La migración de las comunicaciones venezolanas de las llamadas tradicionales y los SMS a aplicaciones de mensajería cifrada representa una importante adaptación defensiva por parte de las poblaciones vulnerables a la vigilancia. Si bien las llamadas por teléfono celular siguen siendo un método de comunicación común, las llamadas de audio y video a través de WhatsApp y Signal ha reemplazado cada vez más a la telefonía tradicional, especialmente entre activistas, periodistas, miembros de la oposición y organizaciones de la sociedad civil conscientes de los riesgos de intercepción. Esta migración limita considerablemente el valor de inteligencia que la intercepción de telecomunicaciones puede proporcionar más allá de los datos de geolocalización y otros metadatos, pues las plataformas de mensajería cifrada de extremo a extremo impiden el acceso al contenido incluso cuando los proveedores de telecomunicaciones cooperan con las solicitudes de vigilancia.

La mensajería cifrada de WhatsApp se ha convertido en la plataforma digital más utilizada en Venezuela, con casi 15 millones de usuarios —más de la mitad de la población del país— que se conectan diariamente.[130] La plataforma sirve como infraestructura de comunicación principal para las actividades cotidianas de los ciudadanos y, cada vez más, para el consumo de noticias políticas. La transición del debate público de las plataformas abiertas de redes sociales a grupos semi privados de WhatsApp surgió en respuesta a factores económicos (menor consumo de datos) y políticos (menor riesgo de represalias inmediatas). Los debates públicos han migrado a los grupos de WhatsApp, donde líderes políticos, periodistas, defensores de derechos humanos, activistas sociales y académicos interactúan con menor riesgo de exposición, pues los chats cifrados y privados de la plataforma, en teoría, protegen las conversaciones de la vigilancia gubernamental directa.

Sin embargo, la intercepción de telecomunicaciones aún puede comprometer las plataformas de mensajería cifrada al explotar los sistemas de autenticación basados en SMS, como se explica en el informe en la siguiente sección sobre infiltración de comunicaciones. Muchas plataformas de mensajería utilizan códigos de verificación SMS para verificar la propiedad de los números de teléfono y proteger las cuentas, lo que crea una vulnerabilidad cuando los proveedores de telecomunicaciones facilitan la intercepción de contenido SMS. La persistencia de vulnerabilidades de autenticación basadas en SMS socava la seguridad que las aplicaciones por mensajería cifrada y otras plataformas en línea pueden ofrecer. Las organizaciones que operan bajo condiciones de máxima vigilancia reconocen cada vez más esta debilidad, utilizando claves (PINs) de autenticación de dos factores en aplicaciones de mensajería y en otras plataformas códigos basados en aplicaciones o llaves físicas (FIDO) para la autenticación de dos factores en lugar de códigos SMS. Sin embargo, la sofisticación técnica requerida para estas medidas de protección, combinada con recursos limitados de alfabetización digital y una conectividad a Internet poco fiable, genera vulnerabilidades asimétricas, dejando a las poblaciones más vulnerables sin la capacidad de implementar defensas efectivas.

Vigilancia del tráfico de Internet

Más allá de interceptar las telecomunicaciones tradicionales, las autoridades venezolanas poseen capacidades para la vigilancia, manipulación y censura del tráfico de Internet. CANTV, la empresa estatal de telecomunicaciones que opera como el principal proveedor de servicios de Internet residencial de Venezuela, ha desplegado equipos de red avanzados capaces de analizar el tráfico, implementar censura, manipular y alterar el tráfico y monitorear las comunicaciones de Internet sin cifrar. El alcance total de esta capacidad de vigilancia del tráfico aún no está claro, pero los incidentes documentados indican que se ha desplegado contra objetivos políticamente sensibles.

Las capacidades técnicas del proveedor estatal CANTV, junto con la total falta de supervisión independiente, crean un entorno propicio para la vigilancia exhaustiva de Internet sin documentación pública ni rendición de cuentas. La manipulación del tráfico de red por parte de CANTV para facilitar ataques de phishing (descritos en la sección de ciberataques de este informe) se basa en equipos de red avanzados que también se utilizan para analizar el tráfico de Internet. Estos equipos están diseñados para facilitar la censura sofisticada de Internet, alterar el tráfico o vigilar las comunicaciones de Internet sin cifrar. Aún no se sabe con certeza si este tipo de vigilancia del tráfico de red se utiliza actualmente ni en qué medida.

Los proveedores privados de servicios de Internet enfrentan una intensa presión para cooperar con las solicitudes de vigilancia, dada la autoridad regulatoria de CONATEL (la Comisión Nacional de Telecomunicaciones) sobre licencias, asignación del espectro y permisos operacionales. Si bien el informe de transparencia de Telefónica incluyó el tráfico de Internet en sus estadísticas de intercepción sin proporcionar un desglose claro por tipo de solicitud, la falta de datos granulares hace que sea imposible determinar de manera definitiva si las autoridades venezolanas solicitaron o recibieron sistemáticamente contenido de tráfico de Internet de proveedores privados.

Rastreo de ubicación y captadores IMSI

El rastreo de ubicación a través de la infraestructura de telecomunicaciones representa una capacidad de vigilancia distinta pero relacionada que las autoridades venezolanas pueden implementar estratégicamente. El mandato del Código de Procesamiento Penal que exige que las instituciones financieras y de telecomunicaciones mantengan disponibilidad 24/7 para “procesar y proporcionar el registro de ubicación de los ciudadanos” crea una infraestructura de rastreo permanente y en tiempo real accesible a una amplia gama de entidades autorizadas.[131] Los datos de intercepción de telecomunicaciones que pueden solicitar las autoridades venezolanas incluyen información de ubicación celular generada cuando los teléfonos móviles se conectan a las torres de telefonía celular. Estos datos pueden permitir registros detallados de movimiento que revelan información sobre asociaciones, actividades, visitas a lugares sensibles y relaciones de individuos inferidas a través de patrones repetidos de co-ubicación.

Más allá de esta cooperación con proveedores de telecomunicaciones autorizados, la evidencia técnica indica el despliegue de dispositivos de vigilancia celular no autorizados, conocidos como receptores IMSI, Stingrays (llamados así por el nombre de un fabricante destacado) o simuladores de estaciones base. Estos dispositivos suplantan la identidad de torres de telefonía móvil legítimas, lo que provoca que los teléfonos móviles cercanos se conecten a ellas y revelen directamente qué teléfonos están presentes en un área geográfica. Esta tecnología permite localizar a personas específicas dentro de áreas limitadas y, potencialmente, interceptar el contenido de las llamadas y los mensajes de texto que se producen cerca de la antena falsa, todo sin la cooperación ni el conocimiento del proveedor de telecomunicaciones. A diferencia de los datos de ubicación históricos que reconstruyen movimientos pasados, el acceso a la ubicación en tiempo real permite una vigilancia dinámica. Las fuerzas de seguridad pueden usar este recurso para rastrear la ubicación de los objetivos, determinar quién estuvo presente en eventos específicos o identificar personas que se reúnen con personas de interés particulares.

El Proyecto de Detección de Antenas Falsas (FADe por sus siglas en inglés) documentó evidencia técnica de antenas celulares que presentaban inconsistencias, sugiriendo que eran falsas, en Caracas y a lo largo de la frontera entre Venezuela y Colombia durante una investigación realizada en 2019.[132] Si bien la evidencia técnica observada no siempre puede identificar definitivamente al operador o la intención detrás de cada antena anómala, las antenas falsas parecían concentradas en lugares de seguridad estratégicamente significativos, incluido Fuerte Tiuna (la principal base del Ejército de Venezuela donde fue capturado Nicolás Maduro), Plaza Venezuela, puntos de acceso vehicular a Caracas y aeropuertos. [133]Estas ubicaciones sugieren fuertemente un despliegue por parte de instituciones de seguridad para obtener datos directos y en tiempo real sobre ubicación y comunicaciones, posiblemente por parte de unidades especializadas dentro de las fuerzas de seguridad estacionadas en estas zonas.

A diferencia de la intercepción de telecomunicaciones facilitada por la cooperación con proveedores, los operadores de receptores IMSI mantienen acceso directo, continuo y en tiempo real sin depender de entidades externas, sin esperar el procesamiento de la respuesta ni afrontar la remota posibilidad de que una solicitud no se procese. Esta capacidad autónoma ofrece ventajas tácticas para operaciones urgentes como arrestos, vigilancia de objetivos de alto valor o monitoreo de ubicaciones sensibles. La concentración de antenas anómalas en instalaciones militares, centros de transporte y zonas propensas a protestas sugiere un despliegue operativo alineado con las prioridades de protección del régimen, más que con fines generales de aplicación de la ley.

Ciberataques, infiltración y software malicioso

El marco legal venezolano ofrece protecciones nominales contra los delitos cibernéticos y el acceso no autorizado a las comunicaciones, pero las violaciones sistemáticas por parte de actores estatales hacen que estas salvaguardas carezcan de sentido en la práctica. La Ley Especial Contra Delitos Informáticos de 2001 estableció sanciones penales por acceso no autorizado, intercepción de comunicaciones y divulgación indebida de datos personales, con penas de prisión que van de tres a cinco años por las violaciones.[134] La Ley de Protección de la Privacidad de las Comunicaciones de 1991 refuerza principios de inviolabilidad que exigen autorización judicial para cualquier intercepción y limitan la vigilancia legal a delitos específicos, incluidas las amenazas a la seguridad del Estado, el tráfico de estupefacientes y el secuestro. [135]Estas protecciones, no obstante, existen solo en el papel. Venezuela carece de una legislación integral de protección de datos que se ajuste a los estándares internacionales y la Ley de Transparencia de 2021, en lugar de garantizar la rendición de cuentas, consolidó aún más el secretismo y la impunidad gubernamental. L[136]a subordinación del poder judicial al poder ejecutivo elimina una supervisión significativa de las actividades de vigilancia, mientras que las fuerzas de seguridad obligan regularmente a los ciudadanos a borrar contenidos o extraer datos de sus dispositivos sin autorización legal.

Este vacío regulatorio permite el despliegue sistemático de ciberataques sofisticados contra disidentes, periodistas y organizaciones de la sociedad civil. Además de la intercepción masiva de telecomunicaciones realizada con la cooperación de proveedores de telecomunicaciones, los actores estatales venezolanos emplean técnicas sigilosas para acceder a comunicaciones privadas y rastrear objetivos, incluyendo campañas de phishing para comprometer cuentas en línea, infiltración no autorizada en plataformas organizacionales que contienen información confidencial y robo de cuentas en aplicaciones de mensajería. Estas operaciones suelen coordinarse con campañas de desinformación e infraestructura de censura de Internet, amplificando su impacto mediante ataques simultáneos en múltiples frentes. La magnitud y la sofisticación de los incidentes documentados demuestran una política estatal deliberada, más que una actividad delictiva aislada.[137]

Esta sección examina tres categorías de ciberataques y técnicas de intrusión digital empleadas contra la sociedad civil venezolana. La primera subsección documenta operaciones de phishing desde el Estado, incluyendo campañas masivas dirigidas a iniciativas de la oposición como Voluntarios por Venezuela, Héroes de la Salud y unidades de organización electoral denominadas comanditos, así como ataques dirigidos contra periodistas y objetivos individuales de alto valor. Estas campañas combinan sofisticación técnica con la coordinación entre múltiples entidades gubernamentales. La siguiente sección analiza el acceso no autorizado a plataformas sensibles y cuentas de mensajería, incluyendo casos documentados de apropiación de cuentas explotando las capacidades de intercepción de telecomunicaciones. La tercera sección aborda la implementación de software espía, examinando los esfuerzos persistentes de Venezuela por adquirir herramientas de vigilancia comercial y la evidencia limitada pero preocupante de su uso activo contra defensores de derechos humanos.

Phishing dirigido a periodistas y activistas pro democracia

El phishing representa la categoría más común y mejor documentada de ciberataques patrocinados por el Estado en Venezuela.[138] Los ataques, claramente atribuibles a actores gubernamentales, han utilizado sitios web falsos que imitan iniciativas de la oposición para identificar a activistas, voluntarios y disidentes a gran escala, dejando rastros técnicos que permiten una atribución definitiva a la infraestructura estatal. En muchos casos documentados las personas expuestas se enfrentan a la identificación pública como castigo y las personas que podrían participar en iniciativas similares se ven intimidadas, y en paralelo, se erosiona de modo deliberado la confianza en las organizaciones de la oposición. Todo a través de campañas coordinadas de desinformación que amplifican datos robados.

Voluntarios por Venezuela

En febrero de 2019, durante la crisis constitucional tras la juramentación de Juan Guaidó como presidente interino, la oposición anunció una iniciativa voluntaria para canalizar ayuda humanitaria a Venezuela. VEsinFiltro detectó una campaña de phishing a gran escala dirigida a personas que intentaban registrarse en voluntariosxvenezuela.com. El objetivo principal de la operación era obtener información personal de ciudadanos que creían registrarse en el portal legítimo. El ataque requirió la coordinación entre el aparato de censura de Internet, las redes de desinformación y múltiples entidades estatales.[139]

El ataque implicó una combinación de typosquatting, censura en Internet y una campaña coordinada en redes sociales. Se aprovechó de la confusión de los usuarios sobre cómo acceder al sitio legítimo, dirigiéndolos a una URL maliciosa. Este sitio web fraudulento era casi idéntico al original, utilizando el dominio voluntariosvenezuela.com en lugar del legítimo voluntariosxvenezuela.com.

La sofisticada técnica empleada por CANTV, el principal proveedor de servicios de Internet residencial estatal de Venezuela, contaba con una inyección de respuesta DNS. Mediante la manipulación del tráfico, CANTV interceptaba solicitudes DNS de los dispositivos de los usuarios que buscaban la dirección IP del sitio legítimo y falsificaba respuestas que los dirigía a una infraestructura maliciosa.[140] Esto excedió las capacidades de la suplantación de DNS simple, afectando cualquier solicitud de DNS a voluntariosxvenezuela.com, incluyendo aquellas de usuarios que utilizan DNS públicos (Google, Cloudflare y Quad9), resolutores privados o direcciones IP directas. La manipulación se realizó mediante un equipo middlebox dentro de la infraestructura de CANTV que inspeccionaba todo el tráfico saliente del ISP.

La atribución directa a CANTV fue posible gracias a la documentación de sofisticadas técnicas de inyección de DNS que requieren el control de la infraestructura de telecomunicaciones. La investigación también documentó la participación de CONATEL (la Comisión Nacional de Telecomunicaciones) mediante evidencia en los registros WHOIS de múltiples dominios utilizados durante la operación de phishing y a través de la respuesta de la institución al incidente.[141] La investigación documentó que otros sitios de phishing eran operados por los mismos actores y se habían utilizado previamente para robar credenciales de Gmail, Twitter (ahora X), Facebook y Hotmail, entre otros servicios. Estos dominios de phishing se registraron con un seudónimo asociado a números de teléfono pertenecientes a líneas oficiales de CONATEL.

Cuando el ataque fue expuesto en las redes sociales, la información del registrante fue modificada en los registros WHOIS públicos en NIC.ve. La coordinación entre los aparatos de censura en momentos críticos cuando la operación de phishing fue suspendida y reactivada utilizando diferentes dominios, combinada con la coordinación con portales y redes de desinformación alineados con el Estado, evidenció aún más la orquestación estatal.

La exposición pública de miles de víctimas de phishing se produjo en un contexto en el que la divulgación de la afiliación política conlleva riesgos materiales de discriminación y represalias, incluido el histórico precedente de la Lista Tascón utilizada para la política sistemática de discriminación durante el gobierno de Chávez 2004 a 2012.[142] Además de socavar la confianza en el liderazgo de la oposición, la campaña generó miedo deliberadamente y buscó desacreditar a periodistas e investigadores digitales, entre quienes se incluye el coautor de este informe, Andrés Azpúrua.[143]El ataque violó de modo simultáneo el derecho a la privacidad, a la libertad de asociación, a la participación política, y en paralelo, causó efectos intimidatorios.

Héroes de la Salud

El 26 de marzo de 2020, CANTV engañó a usuarios inyectando respuestas DNS maliciosas dirigidas a los sitios web heroesdesaludve.info y saludvzla.com. Esta manipulación dirigía a quienes visitaban estos sitios a réplicas falsas diseñadas para capturar su información personal.[144] Es posible que muchos usuarios hayan llegado a estos sitios maliciosos después de hacer clic en enlaces compartidos a través de diversos canales.

La iniciativa legítima, lanzada por el gobierno interino de Juan Guaidó, buscaba brindar asistencia financiera al personal sanitario que enfrentaba condiciones difíciles debido a la pandemia, además de abordar el problema de los salarios persistentemente bajos en el sector público. Según VEsinFiltro, decenas de miles de personas probablemente enviaron su información al sitio web clonado, considerando el amplio alcance y la movilización de la campaña, además de la importante participación de CANTV en el tráfico de Internet venezolano.

Unidades organizadoras electorales de base (comanditos)

Durante la campaña electoral presidencial de 2024, una operación de phishing se dirigió a simpatizantes de la oposición y voluntarios que buscaban registrarse en los comanditos, que constituían grupos locales de movilización electoral. La operación distribuyó un formulario de registro falso, promocionado por cuentas fraudulentas en redes sociales y canales de mensajería, utilizando el enlace acortado malicioso bit.ly/Comandito en lugar del legítimo bit.ly/Comanditos.[145]

La operación empleó typosquatting, utilizando enlaces casi idénticos para inducir comportamientos erróneos, y entregó formularios de registro que ocultaban la diferenciación de URL. La clonación de recursos implementó el formulario a través de la plataforma legítima Google Forms, aprovechando la confianza generalizada en la plataforma y la dificultad de identificar su origen únicamente mediante la inspección del URL. La amplificación de redes y grupos se basó en cuentas de X, Instagram, TikTok y Telegram que promovían el enlace malicioso, se hacían pasar por simpatizantes de la oposición y participaban en otras actividades de desinformación.

El enlace malicioso redirigía a una réplica del formulario original alojado en Google Forms. El formulario fraudulento solicitaba información personal y obligaba a recopilar las direcciones de correo electrónico de los usuarios, añadiendo una pregunta adicional de sí o no: “¿Apoyarías actividades callejeras?”, lo que sugiere interés enfocado en perfilar a las víctimas dispuestas a participar en protestas.

Cazadores de Fake News identificó una red de al menos 45 cuentas falsas en X, controladas por actores pro gubernamentales y activas desde 2023. Estas cuentas participaron en el ataque de phishing promoviendo el enlace malicioso para engañar a seguidores de la campaña de la oposición y exponerlos al registrarse a través del formulario falso.[146]

La campaña de phishing expuso la identidad de voluntarios y simpatizantes, a la vez que permitió la elaboración de perfiles políticos. La pregunta adicional sobre “actividades callejeras” indica el mapeo de la disposición a protestar para posibles represalias. Más allá de las violaciones de la privacidad, la operación atacó el derecho de asociación de los venezolanos derechos y saboteó la organización electoral.

Periodistas y otros objetivos de alto valor

A lo largo de los años, hubo varios casos de phishing dirigidos contra periodistas y organizaciones de la sociedad civil que buscaban obtener credenciales de acceso a cuentas de correo electrónico, redes sociales y WhatsApp. Estos ataques provienen de diversos actores maliciosos, incluidos aquellos asociados con el régimen. Actores asociados al régimen han utilizado phishing y otras técnicas para acceder a cuentas de correo electrónico y luego divulgar su contenido a través de medios de comunicación oficiales o cuentas de redes sociales para publicar mensajes a favor del régimen o desacreditar a figuras de la oposición.

Durante un solo fin de semana, en septiembre de 2024, Espacio Público documentó dos ataques de phishing con objetivos específicos. El 14 de septiembre de ese año, el periodista Andrés Rojas Jiménez recibió mensajes de phishing que solicitaban sus credenciales de Instagram.[147] La misma organización informó que la actriz y escritora Prakriti Maduro fue blanco de un ataque de phishing el 12 de septiembre, lo que resultó en la pérdida de acceso a su cuenta en X. Este ataque ocurrió después de que compartiera testimonios sobre detenciones arbitrarias que otros usuarios le enviaron a través de X el contexto de las protestas post electorales.[148]

Los recientes ataques de phishing contra periodistas y otros actores cívicos han comenzado a fallar gracias a una mayor conciencia general, la adopción de la autenticación de dos factores y los mecanismos de respuesta rápida en colaboración con organizaciones que brindan apoyo en seguridad digital. Sin embargo, los intentos de phishing contra ciertas figuras de alto perfil persisten.

Acceso no autorizado a cuentas y otros ciberataques

Obtener acceso no autorizado a las cuentas de correo electrónico de miembros de la sociedad civil es una práctica recurrente que también afecta a políticos, periodistas y activistas. Como se indicó anteriormente, el phishing dirigido se ha utilizado con frecuencia para obtener acceso no autorizado a cuentas y apropiarse de perfiles en redes sociales, pero VEsinFiltro también ha documentado otros ataques de piratería.

Acceso no autorizado a cuentas de correo electrónico y redes sociales

En otros casos, campañas de acoso por parte de figuras de redes sociales y redes de usuarios afines al gobierno precedieron a intentos de acceder a cuentas, presumiblemente por parte de los mismos actores pro gobierno. En un caso similar, ocurrido en diciembre de 2025, las publicaciones de un usuario de Internet del estado Aragua en X, donde comentaba sobre las tensiones entre Estados Unidos y Venezuela, desencadenaron una campaña de acoso por parte de propagandistas del gobierno, lo que rápidamente derivó en amenazas veladas y doxeo. El acoso que comenzó en X se extendió rápidamente a otras plataformas de redes sociales, WhatsApp y llamadas telefónicas. Agentes conectados con los acosadores intentaron acceder a las cuentas en X y Gmail de la víctima.[149]

Un ejemplo notable de un ataque dirigido involucró al periodista Nelson Bocaranda en 2016. En este incidente, los atacantes tomaron el control de su cuenta de X y accedieron a mensajes confidenciales directos mientras Bocaranda divulgaba información de fuentes gubernamentales anónimas. Para ejecutar el ataque, actores vinculados al Estado obtuvieron una nueva tarjeta SIM para la línea telefónica Movistar de Bocaranda. Esto les permitió recibir códigos de verificación por SMS que usaron para cambiar la contraseña de la cuenta. La adquisición de una nueva tarjeta SIM por parte de los atacantes provocó que la línea de Bocaranda dejara de funcionar en su teléfono; por lo que luego tuvo que solicitar una nueva tarjeta SIM para recuperar acceso a su número.[150]

Robo de cuentas de la aplicación de mensajería

Se han documentado casos de robo de cuentas de WhatsApp pertenecientes a activistas y organizaciones de derechos humanos. Las evidencias, aunque inconcluyentes, sugieren que se pudo haber utilizado la intercepción de telecomunicaciones para ganar acceso. Esto ocurre en un contexto local donde el robo de cuentas de WhatsApp es común en operaciones de phishing con fines delictivos, generalmente para estafar a familiares y amigos de la víctima. Es posible que se hayan encubierto operaciones gubernamentales para simular esquemas delictivos de robo de cuentas y camuflar la acción estatal.

En un caso de 2021, documentado por Conexión Segura y Libre, una organización no gubernamental perdió el control de su cuenta de WhatsApp durante varias horas, una cuenta que se utilizaba para la comunicación con víctimas de violaciones de derechos humanos. Quienes operaban el teléfono afirmaron no haber recibido ninguna solicitud de códigos de registro ni haber sido víctimas de phishing. El incidente ocurrió durante un momento crítico en la investigación del fiscal de la Corte Penal Internacional en el caso de Venezuela. Este incidente probablemente fue perpetrado por agentes estatales que solicitaron el contenido de mensajes SMS al operador móvil para registrar una cuenta de WhatsApp en un dispositivo bajo su control.

En un caso de mayo de 2023 la activista de derechos humanos, Lourdes Ruiz, enfrentó un acceso no autorizado a su cuenta de Instagram, el robo del control de su cuenta en Signal por parte de actores desconocidos, e intentos de acceso a sus cuentas de correo electrónico por varios días. Todo mientras sufría en paralelo el acoso sistemático de las fuerzas policiales. Ruiz había estado recibiendo llamadas intimidatorias de las fuerzas de seguridad y creía que su línea telefónica estaba siendo monitoreada debido a su trabajo documentan-

do violaciones de derechos humanos en centros de detención. Ruiz indicó también que había dejado de usar Signal en ese momento y que no tenía la aplicación instalada. También mantuvo que no recibió ningún mensaje con un código para registrar una cuenta de Signal. Ruiz afirmó que la cuenta de Signal con su número de teléfono fue robada y utilizada para enviar imágenes íntimas –obtenidas de Instagram o de una de sus cuentas de correo electrónico– a al menos una persona conocida de la comunidad de derechos humanos. Se desconoce si las imágenes fueron enviadas a otros contactos.[151]

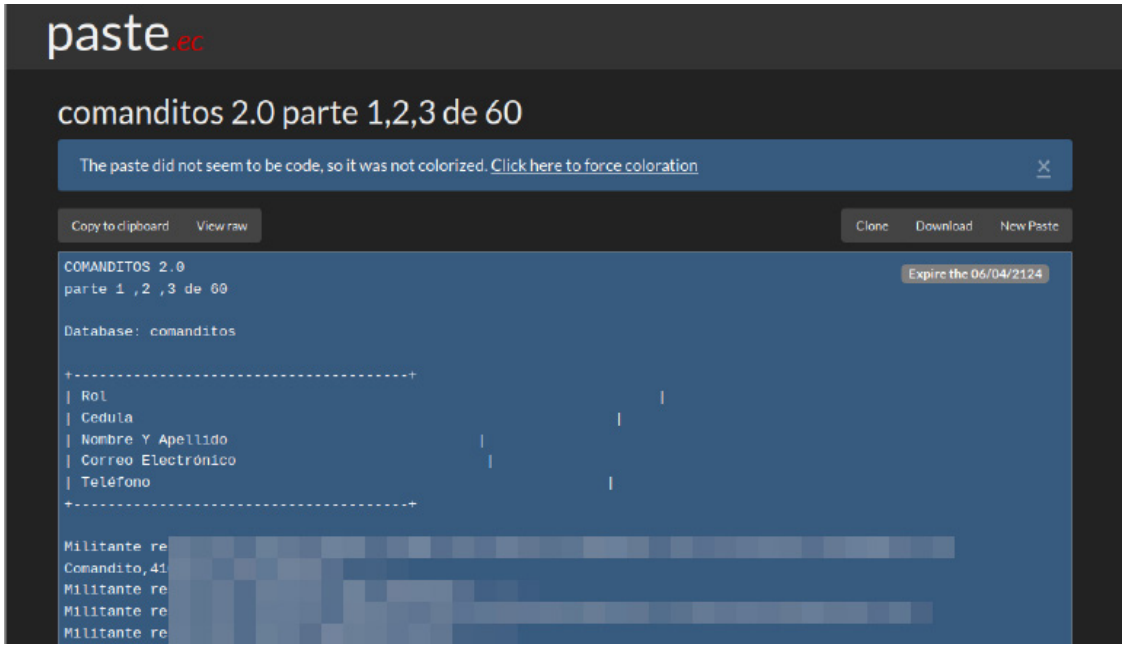
Acceso no autorizado después de detenciones

En algunos casos, las cuentas de personas encarceladas o sometidas a detención temporal fueron vulneradas poco después de su liberación, a veces tras repetidos intentos. Estos ataques probablemente se facilitaron mediante credenciales o dispositivos obtenidos durante los interrogatorios.

En dos casos ocurridos en diciembre de 2025, personas encarceladas perdieron el control de sus cuentas en línea durante la detención o poco después. En un caso, la persona en cuestión perdió el acceso a su cuenta de Facebook y sufrió múltiples intentos fallidos de inicio de sesión por parte de otros actores. Estas situaciones son difíciles de resolver debido a las condiciones de detención, los dispositivos incautados permanentemente por las autoridades y los números de teléfono configurados para la recuperación de cuentas que fueron abandonados en Venezuela antes de una salida rápida o suspendidos por el proveedor de la línea telefónica por falta de uso.

Hackeo de bases de datos

Tanto las víctimas como los perpetradores de ciberataques contra bases de datos estratégicas con frecuencia prefieren no dar a conocer los incidentes. Un caso significativo con fuertes indicadores de participación de actores estatales fue el acceso no autorizado y la divulgación parcial de contenido de la plataforma interna de miembros del partido Primero Justicia durante la campaña presidencial de 2024.

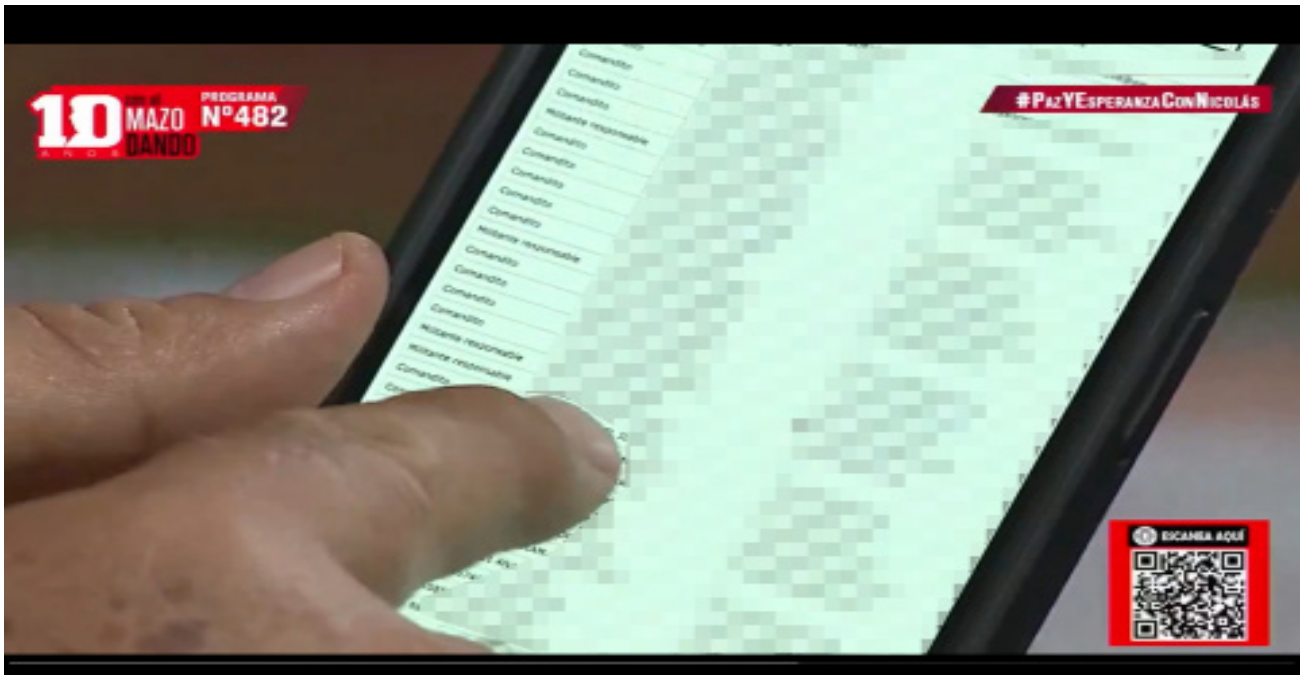


Captura de pantalla de uno de los documentos compartidos por la cuenta de X @LaListaMachado que muestra el registro interno de afiliados a partidos políticos, 27 de junio de 2024. Imagen editada para proteger la privacidad. (Fuente:@LaListaMachado) [78]

El 26 de junio de 2024, Diosdado Cabello, actual ministro de Relaciones Interiores, Justicia y Paz, afirmó en su programa Con el mazo dando que el sitio web comanditos.com había sufrido un hackeo y filtración de su base de datos y mostró en cámara una lista con datos personales de los ciudadanos, incluyendo nombres, cédulas de identidad y direcciones de correo electrónico.[152] Cabello también afirmó: "La confidencialidad de sus datos la ha entregado Maria Corina y su combo", repitiendo una narrativa de desinformación común que ya había sido desplegada por el gobierno durante campañas de phishing. [153]El sitio web comanditos.com fue creado y administrado por el partido opositor Primero Justicia como parte de los esfuerzos para registrar voluntarios durante la campaña presidencial, operando en paralelo con el registro coordinado por el comando de campaña de la oposición y el partido Vente Venezuela, liderado por María Corina Machado. Ambos esfuerzos de los comanditos funcionaron de modo independiente dentro de la coalición democrática.

La cuenta anónima de X, @LaListaMachado, afirmó poseer los datos filtrados. Como en otros casos, narrativas paralelas mezclaron el hackeo y la filtración como fuentes de datos.[154] En los días siguientes la cuenta publicó extensos extractos de bases de datos obtenidas del Sistema de Organización y Registro Electoral (SORE) del Partido Primero Justicia, incluido miembros de los comanditos, listas de miembros del partido y credenciales de inicio de sesión para algunos usuarios con sus contraseñas.

No hay certeza sobre cómo los actores obtuvieron acceso inicial no autorizado al Registro Nacional de Militantes del partido político Primero Justicia y a su base de datos SORE y una atribución definitiva no es posible. VE sin Filtro confirmó que las credenciales expuestas en redes sociales fueron correctamente autenticadas en la plataforma interna del partido Primero Justicia y brindaron acceso a la información recopilada en comanditos.com, que coincide con los datos divulgados por Diosdado Cabello en televisión.[155]



Transmisión #482 de Con El Mazo Dando, 26 de junio de 2024. Imagen editada para proteger la privacidad de las personas que aparecen en la lista filtrada. (Fuente: Con El Mazo Dando)

Este incidente no sólo representa una violación de la privacidad de los ciudadanos cuyos datos se filtraron, sino que también manifiesta preocupaciones más amplias sobre derechos políticos, libertad de asociación y derechos digitales en el contexto político venezolano. Además, la manipulación de la información relacionada con las filtraciones se usa para fabricar cargos criminales o difamar a las víctimas que públicamente por figuras gubernamentales, entre ellas Diosdado Cabello, mostrando un patrón de persecución y deslegitimación de los partidos de oposición.

Señales elusivas de la implementación de software espía

El uso de software espía en dispositivos móviles y computadoras pertenecientes a objetivos de inteligencia estatal ha crecido drásticamente en todo el mundo, incluyendo en Latinoamérica. El software espía generalmente accede a micrófonos, cámaras, contenido del dispositivo (incluidos mensajes) y ubicación en tiempo real, evadiendo medidas de protección de la privacidad como las comunicaciones cifradas, pues se ejecuta directamente en los dispositivos donde se envían o reciben estos mensajes. No ha sido posible identificar completamente el uso de ninguna familia de software espía comercial por parte de las autoridades venezolanas. Sin embargo, casos individuales, interés reiterado y documentado en adquirir software espía, y múltiples inversiones en otros sistemas de vigilancia digital apuntan a su utilización por parte del Estado venezolano.

Durante años, Venezuela ha buscado adquirir software espía sofisticado de varias empresas. Sin embargo, los investigadores no han podido verificar si las compras se ejecutaron finalmente. Queda claro que la comercialización de software espía está rodeada de secretismo, ofuscación e intermediarios. No obstante, es razonable suponer que las empresas que comercializan estas herramientas están especialmente interesadas en ocultar contratos cuando tratan con países sancionados por violaciones generalizadas de derechos humanos o ventas que podrían afectarles negativamente en mercados de alto valor, como Estados Unidos y la Unión Europea.

Entre 2014 y 2015, Citizen Lab encontró evidencia de infraestructura en Venezuela utilizada para alojar servidores de comando y control para el software espía FinFisher, aunque Venezuela no fue mencionada como cliente en una filtración que hubo en la compañía.[156] El servidor de comando y control del software espía FinFisher fue, no obstante, identificado en Venezuela por Citizen Lab en su informe de 2015 y aparentemente se encontraba en Caracas. El hallazgo fue posible gracias al descubrimiento de un servidor proxy con software de la misma empresa, configurado para anonimizar y ofuscar la ubicación del servidor que controla las instancias de spyware. Este conjunto de servidores estuvo operativo entre diciembre de 2014 y octubre de 2015. Su existencia indica que FinFisher fue utilizado por las autoridades venezolanas o, al menos, que se realizó una demostración de campo.

En 2015, una filtración de la ahora desaparecida empresa Hacking Team expuso múltiples conversaciones entre la empresa y el gobierno de Chávez, y posteriormente con el gobierno de Nicolás Maduro.[157] En correos electrónicos filtrados, VenTech, una empresa con oficinas en Caracas y Madrid, afirmó que su "cliente ya cuenta con un presupuesto aprobado para un sistema de intercepción" respecto al software espía Sistema de Control Remoto (RCS). [158]En un correo electrónico anterior del mismo hilo, el representante de la empresa mencionó la posibilidad de colocar el producto en el SEBIN y en la "DIM", refiriéndose a la DGCIM. La filtración no aclara si se realizó un seguimiento, y una investigación de Armando.info no pudo confirmar ni descartar la venta de este sistema a Venezuela.[159]

Documentos obtenidos por periodistas de intelligenceonline.com muestran que la firma 9th Vision, registrada en Sudáfrica, trató de vender software espía al Ministerio del Poder Popular para la Defensa de Venezuela entre 2021 y 2022.[160] Esta empresa ofrece intrusiones sin necesidad de clics, que permiten infectar un dispositivo sin intervención de la víctima. Se informó que las autoridades venezolanas contactaron a otra empresa que comercializaba spyware en 2021, pero no se han confirmado los detalles.

En un caso de 2022 que no se había denunciado anteriormente, Conexión Segura y Libre tuvo un acceso breve al teléfono móvil de una activista de derechos humanos que presentaba síntomas de infección por software espía. Simultáneamente, ella y otros miembros de la misma organización no gubernamental fueron víctimas de acceso no autorizado a cuentas de correo electrónico y otras formas de persecución documentadas, incluyendo llamadas intimidatorias de funcionarios del SEBIN. En este incidente, la víctima denunció que el teléfono mostraba la animación de captura de pantalla del sistema operativo sin interacción del usuario, y que posteriormente las capturas no se encontraron en la galería de fotos. Este comportamiento, junto con otros problemas sin explicación, indican que el software espía no fue optimizado adecuadamente para funcionar sin ser detectado en ese modelo de Android.

Registro e incautación de dispositivos electrónicos

La inspección de teléfonos móviles sin orden judicial por parte de funcionarios estatales venezolanos se ha convertido en una práctica cada vez más generalizada y peligrosa que expone la vida privada de las personas y puede dar lugar a detenciones arbitrarias, extorsión y represalias. Mediante estas inspecciones, las autoridades acceden a información personal, comunicaciones privadas y opiniones políticas sin autorización judicial ni justificación legal, creando un clima de miedo e indefensión. Esta práctica se enmarca en un contexto político más amplio en el que el gobierno autoritario venezolano ha desmantelado sistemáticamente la independencia judicial y el Estado de derecho, transformando a las fuerzas de seguridad del Estado en instrumentos de control político en lugar de servicio público.

Venezuela carece de garantías legales efectivas que protejan a sus ciudadanos de registros arbitrarios de dispositivos electrónicos. La Constitución del país protege nominalmente la privacidad y la correspondencia personal, pero estas garantías se han violado sistemáticamente en la práctica, en particular tras las controvertidas elecciones presidenciales de 2024 y la posterior represión política.[161] La ausencia de procedimientos legales claros que regulen las inspecciones de dispositivos, combinada con una impunidad casi total por los abusos de las fuerzas de seguridad, ha creado condiciones en las que millones de venezolanos se enfrentan a riesgos de vigilancia constante.

La declaración del estado de emergencia el 3 de enero de 2026 incrementó estos riesgos al ordenar a las fuerzas de seguridad encontrar y capturar a cualquiera que "promoviera o apoyara" la operación estadounidense en Venezuela.[162] Esta sección examina los patrones documentados de registros e incautaciones de dispositivos, las tácticas empleadas por los actores estatales y los profundos impactos de estas prácticas en los derechos humanos de la sociedad venezolana.

Documentación sistemática de abusos

Para comprender mejor y documentar sistemáticamente estas prácticas, Conexión Segura y Libre realizó una consulta pública del 7 al 23 de enero de 2026, recopilando denuncias de personas afectadas y de quienes tenían conocimiento directo de los incidentes. La consulta se difundió a través de redes sociales, canales digitales y redes de contacto como un mecanismo accesible y seguro para denunciar estos incidentes en un entorno de alto riesgo, lo que facilita la denuncia de abusos. La consulta sistematizó 58 informes de inspecciones de teléfonos móviles realizadas por funcionarios estatales venezolanos, con incidentes que ocurrieron principalmente entre 2024 y enero de 2026.[163] Los testimonios recogidos no pretenden medir exhaustivamente el fenómeno sino visibilizarlo, identificar patrones de funcionamiento y dar cuenta de cómo las inspecciones telefónicas arbitrarias se han convertido en herramientas de control, intimidación y castigo, con impactos directos sobre derechos fundamentales.

Los incidentes documentados se concentraron en alcabalas informales, puestos de control militar en carreteras y detenciones callejeras aleatorias, especialmente en los estados más poblados del país como Zulia, Miranda, Distrito Capital, Táchira, Carabobo y Bolívar. En la mayoría de los casos, las personas simplemente transitaban por la calle o viajaban entre estados, sin orden judicial ni fundamento legal claro para inspeccionar sus dispositivos móviles. Esta distribución geográfica refleja tanto el despliegue de las fuerzas de seguridad como los cuellos de botella estratégicos donde las autoridades ejercen el máximo control sobre la circulación de la población civil.

Las principales fuerzas de seguridad identificadas como responsables de estos allanamientos son la Guardia Nacional Bolivariana (GNB) y la Policía Nacional Bolivariana (PNB), seguidas de cuerpos policiales estatales o municipales, funcionarios de la Dirección General de Contrainteligencia Militar (DGCIM) y personal uniformado no identificado, algunos encapuchados o vestidos de civil. En la mayoría de los casos, los funcionarios no se identificaron (36 casos) o lo hicieron sólo parcialmente (16 casos), agravando así la arbitrariedad de estas acciones y eliminando cualquier posibilidad de rendición de cuentas.

La información recopilada muestra que en 34 casos hubo una solicitud directa para inspeccionar el teléfono, mientras que en 23 la inspección fue forzada, acompañada de coerción, amenazas de detención, incriminación penal o represalias. Incluso cuando las víctimas indicaron haber "consentido" a la inspección, la mayoría afirmó haberlo hecho por miedo, anulando así cualquier noción de consentimiento libre, previo e informado. Este patrón revela la ficción de la cooperación "voluntaria" en condiciones de vigilancia autoritaria, cuando la negativa conlleva el riesgo de detención, daño físico o, peor aún, el consentimiento pierde su significado. Activistas, periodistas y trabajadoras de la sociedad civil denuncian una especial vulnerabilidad al acoso sexual, la intimidación mediante amenazas contra familiares y formas de coerción específicas de género durante las inspecciones de dispositivos.

Las prácticas de inspección más frecuentes incluyeron el acceso a galerías de fotos y videos, chats de WhatsApp, Telegram y SMS, redes sociales y archivos almacenados en la nube (Google Drive, iCloud, Dropbox). En 29 casos los funcionarios forzaron el desbloqueo del dispositivo y en 14 confiscaron temporalmente los teléfonos o los inspeccionaron fuera de la vista de la persona afectada. Los testimonios reportan repetidamente el uso de búsquedas con palabras clave como "Maduro", "Diosdado", "María Corina", "guarimbero" (un término peyorativo para los manifestantes), "gobierno" o referencias a las elecciones del 28 de julio. Esto sugiere un interés específico en identificar opiniones políticas, conexiones o contenido crítico.

Los funcionarios buscan sistemáticamente pruebas de disidencia, apoyo a la oposición o participación en actividades antigubernamentales. Las búsquedas por palabra clave reflejan las prioridades del régimen y revelan la naturaleza explícitamente política de estas inspecciones. En este contexto, las inspecciones no funcionan como una acción legítima para asegurar el cumplimiento de leyes, sino como operaciones de vigilancia masiva diseñadas para identificar e intimidar a los oponentes políticos.

Un elemento particularmente grave es la extorsión económica asociada a estas inspecciones. Seis informes detallan exigencias de pagos en dólares estadounidenses, en efectivo o por Zelle, como condición para no detener al individuo, no enviar información a las autoridades centrales en la capital, o no imputar a los ciudadanos por delitos graves como terrorismo, incitación al odio o financiamiento ilícito. En estos casos, las cantidades exigidas ascendían a miles de dólares, cantidades fuera del alcance de las personas detenidas, lo que afectaba directamente la integridad, la seguridad económica y la estabilidad familiar de las víctimas.

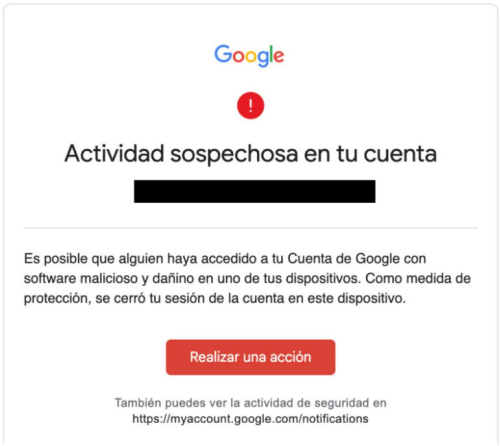
Esta extorsión sistemática transforma la vigilancia en una fuente de ingresos para funcionarios corruptos, a la vez que agrava la instrumentalización política de los registros de dispositivos. Las familias deben elegir entre la ruina financiera y el posible encarcelamiento de sus familiares. Las exigencias en dólares reflejan la dolarización informal de la economía en Venezuela y la explotación de las circunstancias desesperadas por parte de los funcionarios. Para muchos venezolanos, en particular las mujeres, que suelen gestionar la economía doméstica y los recursos familiares, estas exigencias extorsivas crean decisiones imposibles que repercuten en toda la red familiar.

Revisiones enfocadas en individuos de alto perfil en aeropuertos

Personas con perfiles reconocibles en la defensa de derechos humanos, el activismo o el periodismo han sido sometidas a inspecciones de equipos durante interrogatorios que duran horas al entrar o salir de Venezuela a través de los aeropuertos.[164] Estas inspecciones suelen ser mucho más detalladas que las inspecciones sumarias en la calle y abarcan múltiples dispositivos como computadoras portátiles, teléfonos móviles y tabletas. Entre 2023 y 2024, mientras Venezuela se preparaba para las elecciones presidenciales de julio de 2024, al menos siete activistas por los derechos electorales de ONG reconocidas fueron sometidos a interrogatorios en aeropuertos, y al menos cuatro fueron sometidos a inspecciones de equipos, algunos en múltiples ocasiones.

En un caso que involucra a una persona defensora de derechos humanos llevada a interrogatorio en el Aeropuerto Internacional de Maiquetía, que proporcioina servicio a la capital en Caracas, los agentes obligaron al individuo a desbloquear sus dispositivos e inspeccionaron minuciosamente su lista de contactos y chats. Los dispositivos de la persona fueron confiscados y desbloqueados en otra habitación por un período de cuatro

a cinco horas. A las 9:00 am del día siguiente, se recibió una alerta de Google: “Actividad sospechosa en su cuenta: Alguien podría haber accedido a su cuenta de Google usando malware dañino en uno de sus dispositivos”, algo que pudo haber sido provocado por la manipulación de su equipo por parte de los agentes. La alerta indica que las autoridades podrían haber intentado abrir una sesión de Gmail en una computadora del personal de seguridad o haber instalado software malicioso en uno de los dispositivos incautados temporalmente. Como medida de precaución, la persona formateó sus dispositivos y posteriormente aseguró sus cuentas.



Advertencia recibida por persona defensora de derechos humanos horas después del interrogatorio en el que manipularon su equipo sin su supervisión. (Fuente:VE sin Filtro)

Nuevo patrón emergente: búsqueda de individuos en línea

A partir del 3 de enero de 2026, Conexión Segura y Libre documentó múltiples casos en los que las personas reportaron que al llegar a aeropuertos venezolanos, funcionarios de la Policía de Migración les solicitaron sus pasaportes y, antes de permitirles el acceso a las cabinas migratorias, realizaron búsquedas de sus nombres en dispositivos oficiales, principalmente a través de Google Search y buscadores dentro de plataformas de redes sociales. Estas búsquedas parecen tener objetivos similares a las inspecciones de dispositivos móviles: identificar publicaciones con orientación política, establecer posibles conexiones entre individuos o detectar a quienes hayan expresado públicamente su apoyo o celebración de la captura de Nicolás Maduro el 3 de enero.

La búsqueda directa en línea de información sobre viajeros podría constituir una estrategia de vigilancia que intente eludir las medidas de autoprotección digital, como la eliminación de contenidos de los dispositivos personales, así como la negativa a las inspecciones de teléfonos móviles. Aparte de los casos directamente documentados, la consulta identificó 15 informes que abordan específicamente búsquedas por nombre en Google o redes sociales. En cinco de estos casos, las personas indicaron explícitamente que fueron buscadas en Instagram y, en un caso tanto en Google como en Instagram, lo que indica un interés directo en contrastar la identidad y la actividad pública de la persona más allá de la información contenida en el dispositivo móvil.

Violación de la autonomía territorial del campus universitario

El 31 de enero de 2026, el Consejo Universitario de la Universidad Central de Venezuela rechazó públicamente la presencia no anunciada de efectivos policiales y militares en la Ciudad Universitaria de Caracas el 27 de enero durante una visita oficial de la presidente interina Delcy Rodríguez.[165] Según el comunicado institucional, funcionarios de las fuerzas de seguridad intimidaron a los estudiantes mediante revisiones de teléfonos móviles en acciones calificadas como desproporcionadas, intimidatorias y violatorias de la autonomía universitaria y de los derechos fundamentales.[166]

Esta declaración confirma que las inspecciones de dispositivos móviles no se limitan a los puestos de control o a los procedimientos callejeros, sino que se extienden a los campus universitarios, erosionando aún más las fronteras entre la seguridad, el control político y la vida privada. Históricamente las universidades han servido como espacios de autonomía y pensamiento crítico en Venezuela. Su invasión por parte de los aparatos de vigilancia representa una escalada significativa del control autoritario.

Extracción forense y otros medios de extracción de datos del dispositivo

El laboratorio forense digital de la DGCIM es conocido por poseer dispositivos Cellebrite UFED Touch 2 para extraer imágenes forenses de teléfonos móviles y computadoras durante detenciones e investigaciones criminales.[167]No hay información pública disponible sobre qué otras agencias de seguridad tienen estas herramientas de análisis forense.

Las autoridades tienen acceso a equipos para realizar inspecciones más exhaustivas. Estas herramientas de extracción pueden vulnerar la seguridad de algunos teléfonos móviles, dependiendo de su software y configuración, y extraer datos incluso sin conocer la contraseña del teléfono. Conexión Segura y Libre ha visto evidencia de otras formas de extracción de datos de teléfonos móviles, incluidos funcionarios que ubican documentos almacenados en los dispositivos y los envían a sus propios dispositivos usando WhatsApp, extracción de discos duros de computadoras y otros métodos. Este apunta un enfoque oportunista que utiliza cualquier herramienta disponible sin tener en cuenta la integridad, la verificabilidad y la cadena de custodia de los artefactos extraídos.

Efectos generalizados de intimidación sobre el discurso político en espacios con una expectativa razonable de privacidad

El impacto de estas prácticas trasciende el incidente inmediato. Los testimonios reflejan miedo persistente, autocensura, eliminación de aplicaciones, abandono de redes sociales y cambios en las rutinas digitales, adoptados como mecanismos de protección ante posibles inspecciones futuras. Para periodistas, activistas y ciudadanos percibidos como “sospechosos”, estas acciones constituyen una vigilancia intimidatoria que restringe de facto el ejercicio de sus derechos fundamentales. El impacto psicológico se extiende más allá de las personas, a sus familias y comunidades, creando efectos en cascada que multiplican el impacto represivo de cada registro de dispositivo.

La naturaleza sistemática de los registros de dispositivos tiene efectos disuasorios generalizados sobre la participación democrática y la organización de la sociedad civil. Sabiendo que cualquier interacción con las fuerzas de seguridad podría resultar en una inspección telefónica, los venezolanos autocensuran sus comunicaciones y se abstienen de compartir opiniones políticas, incluso en mensajes privados. Esta conformidad anticipatoria representa precisamente el resultado que buscan los regímenes autoritarios: una población que se autocontrola por miedo para reducir la posibilidad de represión directa.

En conjunto, los datos confirman que la inspección arbitraria de teléfonos móviles en Venezuela no constituye un incidente aislado, sino una práctica sistemática y reiterada que combina control, intimidación, castigo y extorsión, en abierta contradicción con las normas nacionales e internacionales de derechos humanos, en particular las relativas a la privacidad, la libertad de expresión y el debido proceso. Esta práctica viola múltiples disposiciones del Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos y las propias garantías constitucionales de Venezuela, que ahora han sido desvirtuadas por las prácticas autoritarias.

La expansión de estas prácticas a campus universitarios, aeropuertos y controles viales demuestra la creciente presión autoritaria sobre la sociedad venezolana. A medida que los espacios tradicionales de relativa autonomía desaparecen bajo la presión de la vigilancia, los venezolanos se enfrentan a decisiones cada vez más difíciles entre la autoprotección digital y la participación social, económica y política normal.

Conclusiones

La coexistencia, incluso sin integración técnica, de diferentes sistemas de vigilancia genera efectos multiplicadores. Por ejemplo, una persona que asiste a una protesta se enfrenta a múltiples riesgos: podría ser identificada mediante cámaras de reconocimiento facial, sus comunicaciones podrían ser interceptadas mientras coordina la asistencia, podría ser víctima de doxeo en redes sociales, sufrir registros de dispositivos en puestos de control y sufrir posibles ciberataques que comprometan sus cuentas digitales. Esta amplia vulnerabilidad transforma la participación política, protegida por la Constitución, en actividades de alto riesgo que requieren sofisticadas medidas de seguridad operativa, alterando fundamentalmente la naturaleza de la participación democrática.

La infraestructura de CCTV de Venezuela se ha convertido de modo sistemático, no en una herramienta para la seguridad pública, sino en un arma para el control político. Los proveedores, compañías chinas –en particular CEIEC, Hikvision y Dahua– dominan la cadena de suministro a pesar de las sanciones internacionales. Las capacidades avanzadas de reconocimiento facial y detección de matrículas, reforzadas además con inteligencia artificial, operan sin protección de la privacidad, supervisión judicial ni mecanismos de consentimiento ciudadano. El sistema de respuesta a emergencias VEN911 integra extensas redes de cámaras, lo que permite la rápida identificación y localización de disidentes, manifestantes y opositores políticos.

La vigilancia con drones se ha convertido en un sofisticado aparato de intimidación que combina capacidades técnicas avanzadas con tácticas de guerra psicológica. Las fuerzas de seguridad venezolanas despliegan drones comerciales, desde modelos compactos DJI para el consumidor hasta modelos avanzados de seguridad pública Autel con capacidades de vigilancia ampliadas, que operan sin marcos legales que regulen su despliegue o supervisión. La visibilidad deliberada de las operaciones con drones, en particular los vuelos nocturnos sobre zonas de protesta y residencias de opositores, tiene un doble propósito: recopilar información sobre patrones de movimiento y participantes, y crear un efecto disuasorio generalizado en las reuniones de naturaleza política.

Los dispositivos de rastreo GPS descubiertos en vehículos de familiares de presos políticos, algunos equipados con funciones de escucha, revelan capas de vigilancia encubierta que requieren acceso físico, pero que proporcionan datos de ubicación y audio ambiental continuos. El despliegue sistemático de tecnologías de vigilancia de movimiento sin autorización judicial socava gravemente la libertad de reunión y asociación, transformando la participación política, protegida constitucionalmente, en actividades que requieren medidas de seguridad operativa y que conllevan un riesgo considerable.

El Sistema Patria es un pilar de la plataforma de control ciudadano en Venezuela, transformando la prestación de asistencia social y el acceso a los servicios públicos en instrumentos para la extracción sistemática de datos y la manipulación política. La base de datos Patria permite la identificación integral y la recopilación de datos a gran escala, con el dominio de la plataforma registrado a nombre del PSUV, en lugar de a cualquier organismo estatal, lo que demuestra la integración operativa entre el aparato estatal y la estructura del partido. El acceso a las prestaciones sociales, que condiciona la subsistencia diaria de millones de ciudadanos al registro obligatorio y al suministro continuo de información personal, crea incentivos permanentes para la autovigilancia. El diseño técnico del sistema permite mapear las relaciones de los usuarios con otras personas e instituciones, lo que permite a los administradores crear redes de conexión detalladas incluso para quienes no son usuarios.

El ciberpatrullaje sistemático en redes sociales y aplicaciones de mensajería, coordinado por el SEBIN, la DGCIM y las fuerzas policiales regionales, se ha convertido en una maquinaria integral de persecución digital que criminaliza la expresión en línea y genera profundos efectos amedrentadores sobre la libertad de expresión y asociación. Canales de Telegram como “Caza Guarimbas VE” compilan y difunden sistemáti-

camente listas de doxeo con nombres, fotografías, direcciones y números de identificación de personas identificadas como simpatizantes de la oposición, lo que facilita el acoso, las represalias e incluso las detenciones posteriores. La "Operación Tun Tun" ejemplificó la integración de múltiples flujos de vigilancia: las funciones de denuncia de VenApp, los grupos de Telegram y las campañas de arresto puerta a puerta se convirtieron en mecanismos coordinados de persecución que generaron una autocensura generalizada en la sociedad venezolana. Los procesos penales derivados del ciberpatrullaje se basan en contenido digital descontextualizado, sin análisis forense técnico o procedimientos adecuados de cadena de custodia, ni evidencia de daños concretos. También aplican disposiciones vagas como la de "incitación al odio" para criminalizar denuncias ciudadanas y opiniones políticas que constituyen un discurso público legítimo. La convergencia de la vigilancia digital, el procesamiento selectivo y la detención arbitraria ha normalizado la autocensura, ha forzado el desplazamiento de periodistas y activistas y ha debilitado la capacidad organizativa de la sociedad civil.

La intercepción de telecomunicaciones a gran escala representa el componente más intrusivo del aparato de vigilancia de Venezuela, con evidencia documentada de prácticas sistemáticas y generalizadas que superan con creces cualquier justificación legítima de las fuerzas del orden. El informe de transparencia de Telefónica de 2021 reveló 1.523.363 líneas telefónicas afectadas y 205.800 órdenes de intercepción, lo que demuestra una vigilancia a escala industrial imposible de justificar mediante investigaciones penales específicas. La infraestructura estatal de CANTV proporciona acceso directo a los datos de telecomunicaciones y a las capacidades de vigilancia del tráfico de Internet, mientras que los proveedores privados enfrentan intensas presiones para cooperar debido a la autoridad regulatoria de CONATEL sobre licencias y operaciones. Del mismo modo, la documentación del Proyecto FADe sobre los receptores IMSI concentrados en lugares estratégicamente significativos, incluidas instalaciones militares y aeropuertos, indica que las instituciones de seguridad los están desplegando para obtener datos directos y en tiempo real sobre ubicación y comunicaciones sin la cooperación del proveedor o incluso sin una posibilidad remota de que se rechace una solicitud.

Los ciberataques patrocinados por el Estado son sistemáticos y están la coordinación entre múltiples entidades gubernamentales. Campañas de phishing a gran escala instrumentalizaron la infraestructura a nivel de ISP de CANTV para la inyección de respuestas DNS, dirigiendo a los usuarios a sitios maliciosos. La coordinación entre el aparato de censura, las redes de desinformación y las entidades estatales revela una orquestación deliberada, con la exposición pública de las víctimas de phishing en contextos donde revelar la afiliación política conlleva riesgos significativos, dado el precedente histórico de discriminación política sistemática.

El acceso no autorizado a plataformas organizacionales y la apropiación de cuentas de mensajería explotan con frecuencia las capacidades de intercepción de telecomunicaciones. Existen casos documentados que demuestran que los códigos de verificación de SMS interceptados permiten el secuestro de cuentas de WhatsApp y la apropiación de cuentas de correo electrónico y redes sociales. Los persistentes esfuerzos de Venezuela por adquirir software espía comercial de múltiples empresas, junto con la identificación por parte de Citizen Lab de la infraestructura de comando y control de FinFisher en Caracas y los casos documentados de síntomas de infección, apuntan a un despliegue activo a pesar del secretismo y la ofuscación que rodean la comercialización de software espía para regímenes sancionados.

La inspección de teléfonos móviles sin orden judicial se ha convertido en una práctica generalizada y peligrosa que combina control, intimidación, castigo y extorsión, en abierta contradicción con las normas nacionales e internacionales de derechos humanos. La sistematización revela una cooperación forzada, ya que las inspecciones se acompañan de coerción y amenazas de detención o procesamiento penal. Las búsquedas de palabras clave como "Maduro", "Diosdado", "María Corina" o referencias a las elecciones del 28 de julio revelan una naturaleza explícitamente política, diseñada para identificar la disidencia en

lugar de servir a fines legítimos de aplicación de la ley. La extorsión económica agrava el uso de armas políticas, con informes que documentan exigencias de miles de dólares en efectivo o transferencias Zelle como condición para no detener a personas o acusarlas de terrorismo o incitación al odio, transformando la vigilancia en una fuente de ingresos para las fuerzas del orden. Personas de alto perfil en los aeropuertos se enfrentan a inspecciones de equipos que duran horas, mientras que los patrones emergentes incluyen búsquedas en línea de los nombres de los viajeros en Google y redes sociales para encontrar información sobre las opiniones políticas de los ciudadanos comunes.

En conjunto, estos hallazgos demuestran que la infraestructura de vigilancia venezolana opera como un sistema integrado de control autoritario que trasciende tecnologías individuales o actores institucionales. La convergencia de la videovigilancia con la intercepción de telecomunicaciones, el ciberpatrullaje con el registro de dispositivos y las aplicaciones estatales con los ciberataques genera efectos multiplicadores que limitan gravemente el espacio cívico y alteran el cálculo de riesgos para la participación política. Los impactos en los derechos humanos se extienden mucho más allá de las violaciones inmediatas y generan profundas transformaciones sociales: la normalización de la autocensura, la erosión de la confianza comunitaria, el desplazamiento forzado de periodistas y activistas, y la conversión de la participación política, protegida por la Constitución, en actividades de alto riesgo que requieren una seguridad operativa sofisticada.

La infraestructura de vigilancia permanece operativa e intacta a pesar de la captura de Maduro el 3 de enero de 2026. Comprender estos sistemas en toda su complejidad, incluyendo sus capacidades técnicas, cadenas de suministro, operadores institucionales, marcos legales e impactos en los derechos humanos, resulta esencial para apoyar a la sociedad civil venezolana en condiciones de máxima represión, fundamentar las respuestas políticas internacionales que aborden tanto los abusos actuales como los futuros mecanismos de rendición de cuentas y, en última instancia, contribuir a las condiciones necesarias para una auténtica transición democrática que incluya el desmantelamiento del propio aparato estatal de vigilancia.

Recomendaciones

Las siguientes recomendaciones abordan las necesidades urgentes de las personas más vulnerables a la vigilancia. También identifican medidas concretas que los gobiernos y las organizaciones internacionales pueden tomar para limitar la infraestructura de vigilancia de Venezuela, proteger a los defensores de derechos humanos, apoyar la seguridad operativa de la sociedad civil venezolana y establecer mecanismos de rendición de cuentas para los proveedores de tecnología que facilitan violaciones sistemáticas de derechos humanos. Estas recomendaciones se derivan directamente de casos documentados, sistemas de vigilancia desplegados, vulnerabilidades técnicas identificadas, dependencias en la cadena de suministro y las realidades operativas que enfrentan los activistas en condiciones de severa represión.

Para las organizaciones de la sociedad civil

- Mejorar el intercambio de datos y mecanismos de monitoreo que documentan el despliegue de tecnología de vigilancia y sus impactos en los derechos humanos en Venezuela a través del despliegue de expertos técnicos. Coordinar la recopilación de pruebas y producir informes públicos periódicos sobre la evolución de la infraestructura de vigilancia bajo la administración interina de Rodríguez. Aumentar la conciencia pública y permitir medidas de protección mediante el intercambio de información, aumentando la conciencia de las mitigaciones contra la vigilancia, identificando áreas de puestos de control de alto riesgo y desarrollando contramedidas con el apoyo de personas expertas.
- Adoptar y poner a disposición formación y recursos de seguridad digital personalizados a diversos grupos de población, incluidos periodistas, activistas y miembros de la oposición, con especial atención a las mujeres en roles de liderazgo, mediante el desarrollo de protocolos específicos para cada contexto que aborden la intercepción de telecomunicaciones, los riesgos de incautación de dispositivos, las amenazas de phishing y la vigilancia de las redes sociales a medida que ocurren las amenazas en Venezuela.
- Establecer redes de respuesta a emergencia para brindar asistencia inmediata cuando los activistas enfrenten detenciones, confiscación de dispositivos o ciberataques selectivos. Coordinar apoyo legal, proteger las comunicaciones, facilitar la reubicación segura cuando sea necesario y generar presión internacional a través de documentación rápida compartida con misiones diplomáticas, organismos internacionales de derechos humanos y redes de medios de comunicación.
- Abogar por que las plataformas tecnológicas implementen funciones de seguridad mejoradas y mecanismos de denuncia de abusos mediante la interacción directa con aplicaciones de mensajería, empresas de redes sociales y proveedores de servicios en la nube para abordar las amenazas específicas de Venezuela. Las personas defensoras de derechos humanos deben abogar también por que las plataformas implementen mecanismos sólidos de denuncia de abusos para campañas de doxeo y acoso coordinado y que proporcionen una respuesta más expedita en procesos de verificación para restaurar cuentas a usuarios que hayan sido hackeados.
- Exigir responsabilidades a los proveedores de tecnología de vigilancia a través de campañas de documentación, acciones legales y actividades de defensa dirigidas a las empresas que suministran infraestructura represiva. Las organizaciones deben recopilar de modo sistemático cómo tecnologías de vigilancia específica facilitan de modo directo violaciones específicas de derechos humanos documentadas. Esta evidencia respalda la incidencia internacional, campañas por presentación de cuentas de compañías privadas y potenciales acciones legales dentro de marcos internacionales de derechos humanos.

Para activistas en pro de la democracia

- Adoptar protocolos de mitigación de la seguridad y vigilancia digital, incluso para escenarios de emergencia. Establecer redes de apoyo en materia de seguridad con expertos en seguridad digital y organizaciones de derechos digitales. Fortalecer la conciencia y las medidas de protección contra el phishing.

- Usar plataformas de comunicaciones cifradas de extremo a extremo y seguir protocolos claros de seguridad en las comunicaciones. Adoptar medidas de protección para estas plataformas, como la autenticación de dos factores y el uso de PIN en las aplicaciones de mensajería.
- Habilitar y utilizar la autenticación multifactor resistente al phishing, específicamente las llaves de seguridad de hardware y las aplicaciones de autenticación TOTP (contraseña de un solo uso con temporizador), para protegerse contra la intercepción de las telecomunicaciones. Los códigos de verificación basados en SMS deberían eliminarse por completo, pues dependen de una infraestructura de telecomunicaciones susceptible a la intercepción estatal.
- Garantizar la seguridad del dispositivo, que incluye mantener el dispositivo actualizado con el sistema operativo y los parches de seguridad más recientes. Establecer un PIN de al menos seis caracteres, o idealmente una contraseña. Evitar softwares pirateados y cualquier otro software de fuentes no confiables.
- Inspeccionar las partes inferiores de los vehículos si han estado bajo control de las fuerzas de seguridad, y también internamente, en casos que involucren a personas de alto perfil; especialmente si experimentan problemas eléctricos inexplicables.
- Activistas, periodistas y defensores de los derechos humanos, en especial las mujeres, deben considerar su mayor exposición a la vigilancia y adoptar prácticas para aumentar el aislamiento y la protección de sus comunicaciones y cuentas, tanto profesionales como personales, así como contenidos y dispositivos, siempre que sea posible.
- Implementar protocolos de desinfección de dispositivos para la movilidad y los escenarios de alto riesgo. Esto incluye los puestos de control, los aeropuertos, las protestas y las detenciones. Esto mediante la protección del dispositivo, manteniendo un mínimo de contenido sensible en los dispositivos y ocultando lo que no se puede eliminar. Configurar asimismo protocolos o usar dispositivos secundarios para actividades sensibles, así como habilitar el borrado remoto.
- Mantener copias de seguridad seguras de evidencia crítica y registros organizacionales para garantizar la continuidad y la preservación de los datos luego de la confiscación, incautación o destrucción del dispositivo, exportando regularmente la documentación clave a un almacenamiento externo cifrado guardado en ubicaciones seguras.

Para gobiernos democráticos

- Exigir el desmantelamiento de la infraestructura de vigilancia política y la rendición de cuentas por los abusos documentados. Condicionar también el alivio de sanciones y la cooperación económica a reformas concretas en materia de vigilancia, así como el enjuiciamiento de funcionarios responsables de violaciones sistemáticas de derechos humanos y el establecimiento de mecanismos de supervisión independientes.
- Apoyar la capacidad de seguridad digital de la sociedad civil venezolana mediante flujos de financiación específicos, programas de asistencia técnica y de apoyo en infraestructura, proporcionando recursos para comunicaciones seguras, reemplazo de dispositivos tras incautaciones, auditorías de seguridad y capacitación técnica continua, coordinados a través de organizaciones con experiencia en derechos digitales. Los gobiernos deben establecer mecanismos de financiación específicos, separados de la promoción democrática más amplia, destinados específicamente a atender las necesidades de seguridad digital: adquisición de dispositivos e infraestructura de comunicaciones seguras, asistencia técnica de profesionales con experiencia y familiarizados con entornos de alta amenaza, apoyo a programas de capacitación en seguridad continuos, fondos de emergencia para el reemplazo de dispositivos tras confiscaciones, y recursos para auditorías de seguridad de organizaciones vulnerables.
- Liderar iniciativas multilaterales que establezcan normas contra las exportaciones de tecnología de vigilancia a regímenes autoritarios mediante marcos coordinados de control de las exportaciones y requisitos de transparencia en la cadena de suministro.

Para organizaciones internacionales

- Desarrollar marcos de rendición de cuentas para los proveedores de tecnología de vigilancia que permiten violaciones de derechos humanos a través de la investigación de cadenas de suministro, documentando las contribuciones tecnológicas específicas a los abusos documentados y aplicando mecanismos legales conforme al derecho internacional de los derechos humanos, incluyendo posibles recomendaciones de presión y remisiones a los órganos judiciales correspondientes. Esto incluye el mapeo completo de las cadenas de suministro, la documentación de las especificaciones tecnológicas que permiten patrones específicos de abuso (reconocimiento facial, extracción forense, intercepción de telecomunicaciones), el establecimiento de vínculos causales entre las tecnologías suministradas y las violaciones documentadas de derechos humanos, y la búsqueda de rendición de cuentas mediante marcos legales adecuados, incluyendo acciones de rendición de cuentas y el apoyo a litigios civiles contra proveedores cómplices.
- Brindar asistencia técnica a las organizaciones de la sociedad civil venezolana facilitando el acceso a herramientas de seguridad digital y el desarrollo continuo de capacidades mediante alianzas con organizaciones de derechos digitales consolidadas y personas expertas en ciberseguridad familiarizadas con entornos operativos bajo alta amenaza. Esto debe incluir la facilitación de alianzas entre la sociedad civil venezolana y personas expertas internacionales en seguridad, la provisión de recursos para la adquisición de infraestructura segura, la coordinación de programas de capacitación que aborden el panorama de amenazas específico de Venezuela, el apoyo a auditorías de seguridad que identifiquen vulnerabilidades organizacionales y el mantenimiento de relaciones de asesoría continuas a medida que las amenazas evolucionan.
- Coordinar campañas internacionales de promoción dirigidas a las empresas de tecnología de vigilancia a través de foros multilaterales y presión pública, aprovechando las plataformas organizativas para visibilizar la complicidad de los proveedores en violaciones de derechos humanos y movilizar respuestas coordinadas de los Estados miembro, la sociedad civil y el sector privado. Esto incluye la elaboración de declaraciones multilaterales que condenen la complicidad de proveedores, la coordinación de las acciones de los Estados miembro que restrinjan las exportaciones de tecnología, campa;as dirigidas a los accionistas que destaquen riesgos reputacionales, la facilitación de campañas de documentación de la sociedad civil y el aprovechamiento de las plataformas organizativas para generar una atención pública sostenida.
- Integrar las preocupaciones sobre vigilancia en los inofrmes de seguimiento sobre derechos humanos, garantizando que los mecanismos tradicionales de documentación incorporen sistemáticamente las violaciones de derechos digitales, el análisis de la infraestructura de vigilancia y la represión tecnológica en las investigaciones, informes y recomendaciones para Venezuela. Con demasiada frecuencia, las violaciones de vigilancia reciben una atención insuficiente dentro de los marcos tradicionales de derechos humanos centrados en la detención física, la tortura y las desapariciones. Las organizaciones internacionales deben garantizar que los mecanismos específicos de cada país (incluyendo la Misión de Determinación de los Hechos de la ONU sobre Venezuela, los relatores de la Comisión Interamericana y los procesos de monitoreo de la OEA) investiguen sistemáticamente la infraestructura de vigilancia, analicen la represión tecnológica, documenten las cadenas de suministro e integren la experiencia en derechos digitales dentro de todo el trabajo relacionado con Venezuela. Esta integración institucional garantiza que la vigilancia reciba la prioridad adecuada junto con la violencia física y las detenciones arbitrarias.

Estas recomendaciones se centran en las necesidades operativas inmediatas de quienes son más vulnerables al aparato de vigilancia de Venezuela. Describen medidas específicas que los gobiernos y las organizaciones internacionales pueden adoptar para limitar la infraestructura represiva, fortalecer la capacidad de la sociedad civil y exigir responsabilidades a los proveedores de tecnología por su papel en la facilitación de la represión. Implementar estas medidas requiere un compromiso sostenido de diversas partes interesadas, la coordinación entre diferentes organizaciones y el reconocimiento de que la vigilancia es un aspecto clave del control autoritario. Este asunto exige estrategias de respuesta específicas y no tratarse como una preocupación menor dentro de los debates más amplios sobre derechos humanos. Durante este período de transición, los actores internacionales deben tomar medidas decisivas para garantizar que los resultados protejan los derechos fundamentales, en lugar de permitir que las capacidades de vigilancia se fortalezcan bajo el liderazgo del nuevo régimen.

Referencias

1. “Informe de Transparencia en las Comunicaciones 2021” Telefónica, 18 de junio de 2022. https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf..
2. “Hoja informativa: President Donald J. Trump Safeguards Venezuelan Oil Revenue for the Good of the American and Venezuelan People” [El presidente Donald J. Trump protege los ingresos petroleros venezolanos en beneficio del pueblo estadounidense y venezolano” The White House, 9 de enero de 2026. https://www.whitehouse.gov/fact-sheets/2026/01/fact-sheet-president-donald-j-trump-safeguards-venezuelan-oil-revenue-for-the-good-of-the-american-and-venezuelan-people
3. Departamento de Estado de los Estados Unidos “A Statement on U.S.-Venezuela Relations,” [Comunicado sobre las relaciones entre EEUU y Venezuela] 5 de marzo de 2026, https://www.state.gov/releases/office-of-the-spokesperson/2026/03/a-statement-on-u-s-venezuela-relations/
4. Simon Lewis y Patricia Zengerie: “Rubio Says US Plan for Venezuela Is Stability, Recovery, Then Transition” [“Rubio dice que el plan de EE.UU. para Venezuela es estabilidad, recuperación y luego transición”] Reuters, 7 de enero de 2026. https://www.reuters.com/world/us/rubio-says-us-plan-venezuela-is-stability-recovery-then-transition-2026-01-07
5. Iria Puyosa, “Delcy Rodríguez’s untenable balancing act” [El equilibrismo insostenible de Delcy Rodriguez] Atlantic Council, 8 de enero de 2026. https://www.atlanticcouncil.org/dispatches/delcy-rodriguezs-untenable-balancing-act/
6. “Comprehensive Strategic Partnership and Cooperation Agreement between the Russian Federation and the Bolivarian Republic of Venezuela,” [Acuerdo de Asociación Estratégica Integral y Cooperación entre la Federación de Rusia y la República Bolivariana de Venezuela] President of Russia, 7 de mayo de, 2025. http://en.kremlin.ru/acts/news/78304.
7. Hoja informativa: President Trump Restoring Prosperity, Safety, and Security to the United States and Venezuela,” (El presidente Trump [y su trabajo] por la restauración de la prosperidad y la seguridad de EEUU y Venezuela) US Department of Energy, 7 de enero de 2026 https://www.energy.gov/articles/fact-sheet-president-trump-restoring-prosperity-safety-and-security-united-states-and
8. “Russian Companies Forced Out of Venezuela After U.S. Capture of Maduro, Lavrov Says,” [Compañías rusas forzadas a dejar Venezuela después de la captura de Maduro por parte de EEUU] The Moscow Times, 5 de febrero de 2026. https://www.themoscowtimes.com/2026/02/05/russian-companies-forced-out-of-venezuela-after-us-capture-of-maduro-lavrov-says-a91872.
9. El 28 de febrero Estados Unidos e Israel atacaron Irán, lo que resultó en la muerte de varios altos funcionarios iraníes, incluyendo al líder supremo, el ayatolá Alí Jamenei. Al momento de la finalización de este informe, Irán atraviesa una situación de inestabilidad política y la continuidad de sus operaciones en Venezuela y otros países es incierta.
10. “Treasury Targets Iran-Venezuela Weapons Trade,” [El Tesoro apunta al comercio de armas Irán-Venezuela] US Department of the Treasury, 30 de diciembre de 2025. https://home.treasury.gov/news/press-releases/sb0347.
11. “Secretary of State Marco Rubio Before the Senate Committee on Foreign Relations on US Policy Towards Venezuela,” [El Secretario de Estado Marco Rubio ante el Comité de Relaciones Exteriores del Senado respecto a la política estadounidense hacia Venezuela] US Department of State, 28 de enero de 2026. https://www.state.gov/releases/office-of-the-spokesperson/2026/01/secretary-of-state-marco-rubio-before-the-senate-committee-on-foreign-relations-on-u-s-policy-towards-venezuela.
12. “El Ilyushin ha realizado seis vuelos de repatriación de cubanos desde Venezuela tras la captura de Maduro”, 14ymedio, 20 de enero de 2026. https://www.14ymedio.com/cuba/ilyushin-realizado-seis-vuelos-repatriacion_1_1122898.html
13. Marleidy Múñoz y Raúl Medina, “The Footprints of Cuban Intelligence in Venezuela,” [Las huellas de la inteligencia cubana en Venezuela]. El Toque, 20 de agosto de 2024. https://eltoque.com/en/the-footprints-of-cuban-intelligence-in-venezuela.
14. “Transición en Venezuela: Delcy Rodríguez eliminó por decreto programas sociales y entes emblemáticos del entramado chavista”. Infobae, 15 de febrero de 2026. https://www.infobae.com/venezuela/2026/02/15/transicion-en-venezuela-delcy-rodriguez-elimino-por-decreto-programas-sociales-y-entes-emblematicos-del-entramado-chavista/.
15. Justicia, Encuentro y Perdón (@JEPvzla), “Hasta la fecha, se ha logrado verificar…” X, 19 de marzo de 2026 https://x.com/JEPvzla/status/2034758824851042697.
16. Regina García Cano y Megan Janetsky, “Hundreds more in Venezuela say their loved ones are ‘political prisoners’ (Cientos más en Venezuela dicen que sus seres queridos son ‘presos políticos’). The Washington Post, 14 de enero de 2026. https://www.washingtonpost.com/world/2026/01/13/venezuela-prisoners-released-us-maduro-rodriguez/798bed6a-f097-11f0-a4dc-effc74cb25af_story.html.
17. “Bloqueos de Internet en Venezuela” VE sin Filtro, March 12, 2026, https://bloqueos.vesinfiltro.org/.
18. “Venezuela: Graves violaciones de derechos humanos en relación con las elecciones”. Comisión Interamericana de Derechos Humanos, 27 de diciembre de 2024. https://www.oas.org/es/cidh/informes/pdfs/2025/informe-venezuela-graves-violacionesddhh-contexto-electoral.pdf
19. “Rodríguez Torres anuncia instalación de 30 mil cámaras de seguridad en zonas con altos índices de criminalidad”, Diario La Voz, 28 de octubre de 2013. https://diariolavoz.net/2013/10/28/rodriguez-torres-anuncia-instala-

cion-de-30-mil-camaras-de-seguridad-en-zonas-de-incidencia-delictiva/.

20. Los Cuadrantes de Paz son unidades básicas territoriales delimitadas geográficamente que forman parte del Sistema Popular de Protección para la Paz (SP3) y la Defensa Integral de la Nación. Ver "Gran Misión Cuadrantes de Paz" Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz, Gobierno Bolivariano de Venezuela, https://www.mpprijp.gob.ve/biblioteca/cuadrantes.

21. "Sistemas de videovigilancia y atención de emergencias en Venezuela". Transparencia Venezuela, 2022. https://transparenciave.org/wp-content/uploads/2022/01/Sistemas-de-videovigilancia-y-atencio%CC%81n-de-emergencias-en-Venezuela.pdf.

22. "Venezuela cuenta con más de 3 mil cámaras de videovigilancia en todo el país (+VEN 911)," Con el Mazo Dando, June 12, 2025, https://mazo4f.com/venezuela-tiene-mas-de-3-mil-camaras-de-videovigilancia-en-todo-el-pais-ven-911.

23. CON EL MAZO DANDO #554", TVFANB MULTIMEDIA, December 3, 2025, https://www.youtube.com/watch?v=IGvG_jj1Xqw.

24. "El vicepresidente sectorial de Política, Seguridad Ciudadana y Paz, Diosdado Cabello, ha afirmado que las cámaras del 911 están activas en todas las calles del país". Globovisión (@globovision), Instagram, 3 de abril de 2025. https://www.instagram.com/reels/DH_bkKvptcV/.

25. "Instalan cámaras en hospitales públicos de Venezuela para "erradicar" supuestos sabotajes". SWI Suiza, 22 de junio de 2025. https://www.swissinfo.ch/spa/instalan-c%c3%a1maras-en-hospitales-p%c3%blicos-de-venezuela-para-%22erradicar%22-supuestos-sabotajes/89562579

26. "Carmen Meléndez: Instalaremos cámaras inteligentes 'en cada esquina y en cada semáforo en Caracas', El Universal, 15 de agosto de 2025. https://www.eluniversal.com/caracas/212222/carmen-melendez-instalaremos-camaras-inteligentes-en-cada-esquina-y-en-cada-semaforo-en-caracas.

27. "ZTE Smart City Full Solution," ZTE Corporation, consultado el 28 de febrero de 2026. https://www.zte.com.cn/global/solutions/digital_transformation/government/ztesmartcity-fullsolution.html.

28. "ZTE Government Cloud Solution," ZTE Corporation, consultado el 28 de febrero de 2026.

29. "Ministro Cabello: 'Guaicaipuro tiene un sistema de cámaras que es extraordinario'", Alcaldía de Guaicaipuro, 13 de noviembre de 2025. https://alcaldiadeguaicaipuro.gob.ve/2025/11/13/ministro-cabello-guaicaipuro-tiene-un-sistema-de-camaras-que-es-extraordinario/.

30. "Proyecto 'Caracas Inteligente' promete garantizar seguridad en la capital", Correo del Orinoco. 4 de diciembre de 2024. https://www.correodelorinoco.gob.ve/proyecto-caracas-inteligente-promete-garantizar-seguridad-en-la-capital/.

31. Díaz, Floralbert: "Avanzan en la instalación de paradas inteligentes en Caracas" Ciudad CCS. https://www.ciudadccs.info/publicacion/34076. "En trabajo conjunto con el equipo de @caracasinteligente, se lleva a cabo la instalación de un novedoso sistema de circuito cerrado, el cual comprende la colocación de cámaras de seguridad y vigilancia en los diferentes espacios del Terminal La Bandera". INTRAVIALCA (@intavialca_ccs), Instagram, 7 de marzo de 2025. https://www.instagram.com/p/DG6THzchFXK/.

32. "El presidente de la Fundación Caracas Ciudad Inteligente y de la Oficina de Tecnologías de la Información y las Comunicaciones, Ing. Darwin Vargas, participó en la instalación del botón de emergencia en la Plaza de la Victoria, en Plaza Venezuela, Fundación para la Caracas Inteligente (@caracasinteligente), Instagram, 12 de noviembre de 2025. https://www.instagram.com/p/DQ-AQiPjxvr/.

33. "US blacklists 28 Chinese companies and government agencies over Uighur repression," The Guardian, October 8, 2019, [Estados Unidos sanciona a 28 empresas y agencias gubernamentales chinas por represión contra los uigur] 8 de octubre de 2019. https://www.theguardian.com/world/2019/oct/08/us-lists-black-28-chinese-companies-and-government-agencies-over-uighur-repression.

34. "El presidente de la Fundación Caracas Ciudad Inteligente y de la Oficina de Tecnologías de la Información y las Comunicaciones, Ing. Darwin Vargas, participó en la instalación del botón de emergencia en la Plaza de la Victoria en la Plaza Venezuela." Fundación Caracas Inteligente (@caracasinteligente), Instagram, 12 de noviembre de 2025. https://www.instagram.com/reel/DQ-AQiPjxvr/.

35. "Desde nuestro Integral de Seguridad Ciudadana comparto con ustedes algunas de las calles y avenidas que se pueden ver gracias a una inversión importante en cámaras de seguridad" Gustavo Duque (@gustavoduquesaez), Instagram, 12 de agosto de 2025. https://www.instagram.com/reels/DNR0KiPxR_b/

36. Entrevista oficial de seguridad en Caracas que pidió permanecer en el anonimato por razones de seguridad, enero de 2026.

37. Ibid.

38. Entrevista oficial de seguridad en Caracas que pidió permanecer en el anonimato por razones de seguridad, enero de 2026.

39. "El monitoreo de cámaras en el #VEN911Baruta es un sistema de videovigilancia y videoprotección que utiliza una red de cámaras instaladas en puntos estratégicos de las ciudades y vías del país . Este sistema opera de manera centralizada desde los Centros de Comando, Control y Telecomunicaciones (VEN 9-1-1)," Ven911baruta (@ven911baruta), Instagram, 30 de octubre de 2025. https://www.instagram.com/p/DQcl1rZjpE5/.

40. "Desde el Centro de Control Integral de El Hatillo (CCI), se canalizan todas las denuncias en el menor tiempo posible," PoliHatillo (@polihatillo),Instagram, 15 de agosto de 2023, https://www.instagram.com/p/Cv-PMIaLAMX/.

41. "Gobierno Bolivariano fortalece sistema de seguridad con expansión masiva de videovigilancia", Ministerio de Interior, Justicia y Paz (@minjusticia_ve), 20 de diciembre de 2025. https://www.instagram.com/p/DSfy86EEWFm/?img_index=4.

42. YugreilisMartínez, "Las cámaras de seguridad han sido un apoyo para desarticular bandas delictivas en Guaicaipuro", Alcaldía de Guaicaipuro, 26 de septiembre de 2022.

https://alcaldiadeguaicaipuro.gob.ve/2022/09/26/guaicaipuro-seguridad-ciudadana-31/.

43. "Promesa cumplida: Más ojos en la calle para tu tranquilidad", Farith Fraija (@farithf), Instagram, 22 de diciembre de 2025. https://www.instagram.com/p/DSkL6-VjaxK/.

44. "Guaicaipuro tiene un sistema de cámaras que es extraordinario," Alcaldía de Guaicaipuro, 13 de november de 2025.

45. "En materia de seguridad, no se improvisa, hace año y medio pusimos en marcha la instalación de cámaras de seguridad en nuestro municipio", Farith Fraija (@farithf), Instagram, 25 de octubre de 2025. https://www.instagram.com/reels/DQMMsfKDawr/.

46. Farith Fraija, vídeo de TikTok, 23 de octubre de 2025, https://www.tiktok.com/@farithf/video/7564491133028420920.

47. "Inició la instalación de cámaras de videovigilancia en la avenida Bolívar del municipio de Valera, como parte de la Gran Misión Cuadrantes de Paz", Gobierno de Trujillo (@gobtrujillo), Instagram, 6 de marzo de 2024. https://www.instagram.com/reels/C4LZLkJr_i6/.

48. "Gobierno Bolivariano relanza el programa de Buen Gobierno 1x10", Ministerio de Ciencia y Tecnología, 25 de octubre de 2025. https://mincyt.gob.ve/gobierno-bolivariano-relanza-del-1x10-del-buen-gobierno/.

49. "Redes de control: censura y represión digital en las elecciones presidenciales en Venezuela", VE sin Filtro, 26 de marzo de 2025. https://vesinfiltro.org/noticias/2025-03-26-venezuela-represion-digital-elecciones/.

50. "Inició la instalación de cámaras de videovigilancia en la avenida Bolívar del municipio de Valera, como parte de la Gran Misión Cuadrantes de Paz", Gobernación de Trujillo (@gobtrujillo), Instagram, 6 de marzo de 2024. https://www.instagram.com/reels/C4LZLkJr_i6/.

51. "Sistemas de videovigilancia y atención de emergencias en Venezuela", Transparencia Venezuela, enero de 2022. https://transparenciave.org/wp-content/uploads/2022/01/Sistemas-de-videovigilancia-y-atencio%CC%81n-de-emergencias-en-Venezuela.pdf.

52. La Oficina de Seguridad Pública y Seguridad Nacional anuncia la incorporación de sistemas de aeronaves no tripuladas (UAS) y componentes críticos de UAS producidos en el extranjero, así como equipos y servicios enumerados en la sección 1709 de la NDAA del año fiscal 2025, a la lista de la FCC.Comisión Federal de ComunicacionesAviso Público, DA-25-1086A1, 22 de diciembre de 2025,. https://docs.fcc.gov/public/attachments/DA-25-1086A1.pdf.

53. Ibid.

54. "Treasury Sanctions CEIEC for Supporting the Illegitimate Maduro Regime's Efforts to Undermine Venezuelan Democracy" [El Tesoro sanciona a CEIEC por apoyar los esfuerzos del régimen ilegítimo de Maduro para socavar la democracia venezolana], Departamento del Tesoro de EE. UU., 30 de noviembre de 2020. https://home.treasury.gov/news/press-releases/sm1194.

55. MinServicioPenitenciario, "Delegación China comprueba óptimo funcionamiento del Sitesep" ("Chinese Delegation Verifies Optimal Functioning of Sitesep"), YouTube video, December 2, 2018,, https://www.youtube.com/watch?v=e-JRoEuJPmAY

56. Scilla Alecci, "US Blacklists Chinese Companies Linked to Uighur Abuses," [Los Estados Unidos sancionan compañías chinas ligadas a abusos contra los uigur] International Consortium of Investigative Journalists, 28 de mayo de 2020. https://www.icij.org/investigations/china-cables/us-blacklists-chinese-companies-linked-to-uighur-abuses/.

57. "¿Conoces los nuevos botones de emergencia instalados por nuestro alcalde @gustavoduquesaez?", Policía Municipal de Chacao (@polichacao), Instagram, 2 de abril de 2024. https://www.instagram.com/reel s/C5RiA8dOUW0/.

58. "Nos complace anunciar que la Fundación Caracas Inteligente ha implementado botones de pánico en lugares estratégicos de nuestra ciudad", Fundación Caracas Inteligente (@caracasinteligente), Instagram, 18 de diciembre de 2024. https://www.instagram.com/reels/DDu8__iPKO6/.

59. Scilla Alecci, "EE. UU. incluye en la lista negra a empresas chinas vinculadas a abusos contra los uigures", Consorcio Internacional de Periodistas de Investigación, 28 de mayo de 2020.https://www.icij.org/investigations/china-cables/ee-uu-incluye-en-la-lista-negra-a-empresas-chinas-vinculadas-a-los-uigures-abusos/.

60. "KIPOD en Venezuela", BELPOL, 9 de octubre de 2024. https://belpol.pro/es/kipod-v-Venezuela/.

61. "US Treasury Targets Belarusian Support for Russian Invasion of Ukraine" [El Tesoro de EE. UU. apunta al apoyo bielorruso a la invasión rusa de Ucrania]. Departamento del Tesoro de EE. UU., 24 de febrero de 2022,https://home.treasury.gov/news/press-releases/jy0607.

62. Carta del director A. P. Knysh de la empresa bielorrusa 24x7 Panoptes dirigida a Remigio Ceballos, Ministro del Poder Popular para las Relaciones Interiores y Justicia, proporcionada por BELPOL.

63. "Венесуэльский адмирал изучил работу центра мониторинга общественной безопасности ГУВД Минска" [Almirante venezolano estudia la labor del Centro de Monitoreo de Seguridad Pública de la Policía de Minsk"] BelTA, 28 de noviembre de 2023 https://belta.by/society/view/venesuelskij-admiral-izuchil-rabotu-tsentra-monitoringa-obschestvennoj-bezopasnosti-guvd-minska-602226-2023/.

64. Diosdado Cabello afirma que ahora "hay cámaras por todos lados: Pórtense bien, los están viendo" Contrapunto, 17 de julio de 2025. https://contrapunto.com/nacional/gobierno/diosdado-cabello-afirma-que-ahora-hay-camaras-por-todos-lados-portense-bien-los-estan-viendo/

65. "#NoHanPodidoNiPodrán | El Gobierno del presidente Nicolás Maduro viene denunciando los planes fascistas de la ultraderecha y las alianzas con bandas criminales.", Con el Mazo Dando (@ConElMazoDando), X, 7 de agosto de 2025. https://x.com/ConElMazoDando/status/1953605660584935911?s=20

66. Familiares de presos políticos en Zona 7 denuncian la instalación de cámaras de seguridad en el lugar donde están instalados los campamentos donde pernoctan. Cristian Crespo F (@cristiancrespoj), X, 21 de enero de 2026. https://x.com/cristiancrespoj/status/2014110234218815677.

67. Ibid

68. "Sistemas de videovigilancia y atención de emergencias en Venezuela," Transparencia Venezuela, January 2021, https://transparenciave.org/wp-content/uploads/2022/01/Sistemas-de-videovigilancia-y-atencio%CC%81n-de-emergencias-en-Venezuela.pdf.

69. "Reporte Redes de Control: Censura y represión digital en las elecciones presidenciales en Venezuela" VEsinFiltro, julio de 2024. https://vesinfiltro.org/noticias/2025-03-12-reporte-elecciones-presidenciales/.

70. "EVO Max 4T", Autel Robotics, consultado el 27 de febrero de 2026, https://shop.autelrobotics.com/productos/evo-max-4t-Copiar.

71. "Ukraine Acquires 2,000 Autel EVO Max 4T China-Made Drones," [Ucrania adquiere 2.000 drones Autel EVO Max 4T fabricados en China] Army Recognition, 10 de octubre de 2023. https://www.armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/ukraine-acquires-2-000-autel-evo-max-4t-china-made-drones.Hunted from Above: Russia's Use of Drones to Attack Civilians in Kherson, Ukraine," [Perseguidos desde arriba: el uso de drones por parte de Rusia para atacar a civiles en Kherson, Ucrania], Human Rights Watch, 3 de junio de 2025. https://www.hrw.org/report/2025/06/03/hunted-from-above/russias-use-of-drones-to-attack-civilians-in-kherson-ukraine.

72. "Entities Identified as Chinese Military Companies Operating in the United States," [Entidades identificadas como empresas militares chinas que operan en Estados Unidos"] Departamento de Defensa de EE. UU., 7 de enero de 2025, https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTIDADES-IDENTIFICADAS-COMPAÑÍAS-MILITARES-CHINAS-QUE-OPERA-EN-LOS-ESTADOS-UNIDOS.PDF.

73. "Esta imagen es para el mundo: momento máximo de concentración cuando habló la jefa de las protestas vandálicas y violentas. ", Delcy Rodríguez (@delcyrodriguezv), X, 3 de agosto de 2024. https://x.com/delcyrodriguezv/estado/1819823973586153615.

74. "Demostración del efecto de zoom cardán Autel DG-L35T", Autel Robotics, https://www.autelrobotics.com/videos/autel-alfa/.

75. Reporte Redes de Control: Censura y represión digital en las elecciones presidenciales en Venezuela", VEsinFiltro, julio de 2024. https://vesinfiltro.org/noticias/2025-03-12-reporte-elecciones-presidenciales/.

76. "Autel Alpha: Everything you need to know," [Autel Alpha, todo lo que necesitas saber] Advexure, 11 de diciembre 11 de 2024. https://advexure.com/blogs/news/autel-alpha-everything-you-need-to-know.

77. Ibid

78. Ibid.

79. "El régimen de Maduro desplegó drones sobre Caracas para vigilar e infundir terror a los ciudadanos que salgan a protestar,"Infobae, 3 de agosto de 2024. https://www.infobae.com/venezuela/2024/08/03/el-regimen-de-maduro-desplego-drones-sobre-caracas-para-vigilar-e-infundir-temor-a-los-ciudadanos-que-salgan-a-protestar/.

80. "ALERTA Desde hace unas horas, agentes del régimen han rodeado la casa de mi mamá, han puesto alcabalas en toda la urbanización y sobrevolado con drones. También 'se fue' la luz en la zona,"M.C.Machado (@MariaCorinaYA), X, 7 de enero de 2025. https://archive.is/5weYI.

81. "URGENTE!!! Los efectivos de la DAET y del SEBIN asedian la sede de la Embajada de Argentina en Caracas, protegida por Brasil. Ahora, sobrevuelan drones y también bloquean la señal móvil," Pedro Urruchurtu (@Urruchurtu), X, 23 de noviembre de 2024. https://archive.is/EDEYy

82. "Gobierno atribuye explosiones cerca de Miraflores a drones y disparos de advertencia" Sumarium, 6 de enero de 2026. https://sumarium.info/2026/01/05/se-producen-detonaciones-cerca-del-palacio-de-miraflores/.

83. Dispositivo TK-103 documentado por VEsinFiltro mediante la comparación visual del dispositivo.

84. Rastreador GSM/GPRS/GPS para vehículo con tarjeta SIM de 12-24 V CC y control a distancia TK103B ABCLED https://abcled.ee/en/gps-tracker/5349-car-gsm-gprs-gps-tracker-sim-12-24vdc-with-remote-.html

85. "Un dispositivo fue instalado en el vehículo de Margareth Baduel, hija del fallecido general Raúl Isaías Baduel y hermana de Josnars Baduel, durante la jornada de Ruta Global por la Libertad de los Presos Políticos". VPItv (@VPITV), X, 19 de septiembre de 2025. https://archive.ph/aNVky.

86. Kejal Vyas, "General del Ejército venezolano que salvó a Hugo Chávez del golpe muere en la cárcel", The Wall Street Journal, 13 de octubre de 2021. https://www.wsj.com/world/americas/general-del-ejercito-venezolano-que-salvó-a-hugo-chavez-del-golpe-de-estado-muere-en-la-carcel-11634156236.

87. "DENUNCIA URGENTE | Funcionarios no explican la naturaleza del dispositivo puesto en el vehículo de Margareth Baduel durante el cierre de la #RutaGlobalPorLaJusticia, Comité para la Libertad de los Presos Políticos (@clippve), X, 19 de septiembre de 2025. https://archive.is/viejo.

88. Rastreador GPS SinoTrack para vehículos, dispositivo de rastreo GPS 4G LTE, ST-915L, potente rastreador magnético en tiempo real para vehículos, motocicletas, taxis, camiones y autobuses. SinoTrack en Amazon. https://www.amazon.com/SinoTrack-ST-915L-Motocicleta-Impermeable-En-Tiempo-Real/dp/B09K3SKM9F

89. Código Orgánico Procesal Penal. Art 295., http://www.mp.gob.ve/LEYES/CODIGO_OPP/index.html.

90. Iria Puyosa, Andrés Azpurua, and Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," Atlantic Council, julio de 2024. https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

91. Información WHOIS. whois.patria.org.ve, consultado el 24 de mayo de 2024.

92. Andrea Tosta, "El carrusel del PSUV: estocada final al voto secreto," El Estímulo, 19 de diciembre de 2017. https://elestimulo.com/climax/politica/2017-12-19/el-carrusel-del-psuv-estocada-final-al-voto-secreto/.

93. "Lay Sapo", Wikipedia, última modificación: 17 feb 2026. https://es.wikipedia.org/wiki/Ley_Sapo.

94. Iria Puyosa, Andrés Azpurua y Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," [Venezuela: manual digital para la represión] Atlantic Council, julio de 2024. https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

95. Iria Puyosa y Daniel Suárez Pérez, "How the Venezuelan regime weaponized video and messaging apps to persecute dissidents," [Cómo el régimen venezolano está usando aplicaciones de mensajería como armas para perseguir disidentes] Atlantic Council, septiembre de 2024. https://dfrlab.org/2024/09/23/venezuela-weaponizes-apps/.

96. Conexión Venezuela-Panamá: ¿quiénes desarrollaron a VenApp?", Cazadores de Fake News, May 20, 2022, https://www.cazadoresdefakenews.info/conexion-venezuela-panama-quienes-desarrollaron-a-venapp/.

97. "#TeExplicamos | ¿Qué es VenApp y por qué despierta alertas sobre vigilancia y control en Venezuela?", El Diario, 27 de octubre de 2025. https://eldiario.com/2025/10/27/te-explicamos-que-es-venapp-alertas-sobre-vigilancia-y-control-en-venezuela/.

98. "Gobierno pide crear un apartado en Venapp para la vigilancia vecinal", Espacio Público, October 21, 2025. https://espaciopublico.ong/gobierno-pide-crear-un-apartado-en-venapp-para-la-vigilancia-vecinal/#footnote_3_43190.

99. "Manual Redes, Calles, Medios, Paredes y Radio Bemba," 13 de marzo de 2025. https://presidencia.gob.ve/Site/Web/Principal/imagenes/adjuntos/Web/Libros/PDF/Libro95.pdf.

100. Iria Puyosa, Andrés Azpurua y Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," Atlantic Council, julio de 2024. https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

101. John Otis. "Se intensifica la presión contra los medios venezolanos", Comité para la Protección de los Periodistas (CPJ por sus siglas en inglés), 18 de octubre de 2013. https://cpj.org/es/2013/10/se-intensifica-la-presion-contra-los-medios-venezo/

102. "Redes de control: censura y represión digital en las elecciones presidenciales en Venezuela", VE sin Filtro, 26 de marzo de 2025. https://vesinfiltro.org/noticias/2025-03-12-reporte-elecciones-presidenciales/

103. Iria Puyosa y Daniel Suárez Pérez, "How the Venezuelan regime weaponized video and messaging apps to persecute dissidents," [Cómo el régimen venezolano está usando aplicaciones de mensajería como armas para perseguir disidentes] Atlantic Council, septiembre de 2024. https://dfrlab.org/2024/09/23/venezuela-weaponizes-apps/.

104. Ibid.

105. "Redes de control: censura y represión digital en las elecciones presidenciales de Venezuela", VE sin Filtro, 26 de marzo de 2025,https://vesinfiltro.org/noticias/2025-03-26-venezuela-represion-digital-elecciones/.

106. "Redes de control: censura y represión digital en las elecciones presidenciales en Venezuela", VE sin Filtro, 26 de marzo de 2025,https://vesinfiltro.org/noticias/2025-03-26-venezuela-represion-digital-elecciones/.

107. Ibid

108. "Venezuela's military counterintelligence agency posted a chilling video this morning of María Oropeza, a young organizer for the opposition campaign who they arrested on Tuesday." [La agencia de contrainteligencia militar de Venezuela publicó esta mañana un escalofriante video de María Oropeza, una joven organizadora de la campaña de la oposición] Alex Bare (@alexbaretv), X, 8 de agosto de 2024. https://x.com/alexbaretv/estado/1821630754176086487,https://archive.is/PlLu7.

109. "Venezuela: Tech Companies Set Dangerous Precedent with App for Reporting Anti-Government Protesters," [Venezuela: Empresas tecnológicas sientan un precedente peligroso con una aplicación para denunciar a manifestantes antigubernamentales] Amnistía Internacional, 28 de agosto de 2024. https://www.amnesty.org/en/latest/news/2024/08/venezuela-tech-companies-set-dangerous-precedent-with-app-for-reporting-anti-government-protesters/.

110. "Corte de Apelaciones anula condena de 15 años contra estudiante de periodismo Juan Francisco Alvarado." Sindicato Nacional de Trabajadores de la Prensa, 24 de enero de 2026.

111. "Condenan a 30 años de prisión a una doctora por expresarse a través de un audio de WhatsApp,Espacio Público, 18 de noviembre de 2025. https://espaciopublico.ong/condenan-a-30-anos-de-prision-a-una-doctora-por-expresarse/.

112. "Madre de Randal Telles, condenada a 15 años de prisión por un video en TikTok, clama su libertad," Espacio Público, November 22, 2025. https://espaciopublico.ong/madre-randal-telles-condenada-15-anos-video-tiktok-clama-libertad/.

113. "Hermana de Marcos Palma: Nunca pensamos que por la difusión de un audio lo pusieran preso y condenaran," Espacio Público, 22 de octubre de 2025.

114. Históricamente la bandera de Venezuela llevaba siete estrellas que representaban las siete provincias que firmaron la Declaración de Independencia el 5 de julio de 1811. En 2006, el presidente Hugo Chávez ordenó la adición de una octava estrella para simbolizar la provincia de Guayana, que se unió al bando independentista en 1817. La oposición venezolana ha utilizado constantemente la bandera de siete estrellas como parte de un esfuerzo más amplio para impugnar el intento de Chávez de reescribir la historia del país.

115. "Jesús Gabriel Molina Sifontes (27), oficial activo de la Fuerza Armada Nacional Bolivariana y licenciado en Ciencias Navales, fue detenido arbitrariamente el 1 de agosto de 2024 tras culminar sus funciones en el Plan República durante las elecciones presidenciales del 28 de julio," Foro Penal (@ForoPenal), X, 30 de enero de 2026.

116. "Compartir imágenes de recompensas ofrecidas por EEUU le costó la libertad a Rory Branker," Sindicato Nacional de Trabajadores de la Prensa, January 31, 2026.

117. "Conclusiones detalladas de la Misión Internacional Independiente de Determinación de los Hechos sobre la República Bolivariana de Venezuela (A/HRC/57/CRP.5)",

ACNUDH, 15 de octubre de 2024. https://reliefweb.int/report/venezuela-bolivarian-republic/conclusiones-detalladas-de-la-mision-internacional-independiente-de-determinacion-de-los-hechos-sobre-la-republica-bolivariana-de-venezuela-ahrc57crp5 .

118. Constitución de la República Bolivariana de Venezuela (1999), Artículo 60. https://www.constituteproject.org/constitution/Venezuela_2009#s220.

119. Ley Orgánica de Telecomunicaciones, Organización de los Estados Americanos, 28 de marzo de 2000. https://www.oas.org/juridico/spanish/cyb_ven_ley_telecomunicaciones.pdf.

120. Ley de Protección de la Privacidad de las Comunicaciones, 1991. https://venezuela.justia.com/federales/leyes/ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones/gdoc/.

121. "Venezuela: Freedom on the Net—Country Report 2012," Freedom House,, https://freedomhouse.org/sites/default/files/Venezuela%202012.pdf.

122. "Informe de Transparencia en las Comunicaciones 2021" ("Informe de Transparencia en las Comunicaciones 2021"), Telefónica, 18 de junio de 2022. https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf..

123. "El gobierno de Maduro está espiando a los venezolanos a gran escala", VEsinFiltro,22 de junio de 2022. https://vesinfiltro.org/noticias/venezuela-espionaje-comunicaciones/

124. Ibid.

125. "Informe de Transparencia en las Comunicaciones 2021", Telefónica, 18 de junio de 2022. https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf..

126. Iria Puyosa, Andrés Azpurua, and Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," [Venezuela: una guía para la represión] Atlantic Council, julio de 2024. https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

127. "Informe de Transparencia en las Comunicaciones 2021" Telefónica, 18 de junio de 2022. https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf.

128. Ibid.

129. "El gobierno de Maduro está espiando a los venezolanos a gran escala", VEsinFiltro, 22 de junio de 2022. https://vesinfiltro.org/noticias/venezuela-espionaje-comunicaciones/.

130. Iria Puyosa, Andrés Azpurua y Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," [Venezuela: una guía para la represión] Atlantic Council, julio de 2024. https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

131. Código de Procesamiento Penal, Artículo 291. https://tugacetaoficial.com/penal/copp-articulo-291/#:~:text=COPP%20Art%C3%ADculo%20291%20%2D%20C%C3%B3digo%20Penal%20y%20C%C3%B3digo%20Org%C3%A1nico%20Procesal%20 Penal.

132. "Caracas: Faro Sur, Detención de Antena Falsa" y "Frontera colombo venezolana", Proyecto FaDe, marzo de 2020. https://fadeproject.org/?proyecto=caracas y https://fadeproject.org/?project=venezolano-colombiano-borde.

133. Isabel Guerrero, "En estos puntos rojos tu celular es un libro abierto", Armando.info, 6 de septiembre de 2020., https://armando.info/en-estos-puntos-rojos-tu-celular-es-un-libro-abierto/.

134. Ley de Protección de la Privacidad de las Comunicaciones, Venezuela, 2001,https://venezuela.justia.com/federales/leyes/ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones/gdoc/.

135. Ley Orgánica de Telecomunicaciones, Organización de los Estados Americanos, 28 de marzo de 2000. https://www.oas.org/juridico/spanish/cyb_ven_ley_telecomunicaciones.pdf.

136. "Ley de Transparencia aprobada por la Asamblea Nacional consolida secretismo", Transparencia Venezuela, September 17, 2021. https://transparenciave.org/la-ley-de-transparencia-aprobada-por-la-asamblea-nacional-consolida-el-secretismo/.

137. Iria Puyosa, Andrés Azpurua y Daniel Suárez Pérez, "Venezuela: A Digital Playbook for Repression," Atlantic Council, julio de 2024. https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Venezuela-a-playbook-for-digital-repression.pdf.

138. El phishing es un tipo de ataque que busca engañar a la víctima para que lleve a cabo acciones que expongan su seguridad, privacidad, seguridad del dispositivo o para causar pérdidas financieras a través de mensajes, llamadas o sitios web que imitan al de ciertas personas u organizaciones.

139. Andrés Azpúrua y Carlos Guerra, "Phishing del gobierno venezolano pone en riesgo a activistas y usuarios de Internet", VE sin Filtro, 15 de febrero de 2019, https://vesinfiltro.com/noticias/Phishing_by_Venezuelan_government_targets_activists/.

140. Ibid.

141. WHOIS es un protocolo de consulta y respuesta que se utiliza para consultar bases de datos que almacenan usuarios registrados o cesionarios de recursos de Internet, como nombres de dominio y direcciones IP. Consulte la "Especificación del Protocolo WHOIS", RFC 3912, https://www.rfc-editor.org/rfc/rfc3912.

142. La Lista Tascón es una base de datos de venezolanos que firmaron una petición solicitando un referendo revocatorio contra el entonces presidente Hugo Chávez en 2003. Durante años, se utilizó para despedir de empleos en la administración pública a quienes aparecían en ella, negarles servicios públicos y pasaportes, y someterlos a otras formas de discriminación.

143. "Especial IPYS: Bloqueos, robo de datos y contenidos falsos: la nueva forma de interceptar la red venezolana," IPYS Venezuela, 20 de febrero de 2019. https://ipysvenezuela.org/alerta/especial-ipys-bloqueos-robo-de-datos-y-contenidos-falsos-la-nueva-forma-de-interceptar-la-red-venezolana/.

144. "Informe Preliminar: Phishing del gobierno de Maduro contra plataforma Héroes de la Salud" VEsinFiltro, 27 de abril de 2020. https://vesinfiltro.org/noticias/2020-04-26-phishing_heroes_salud

145. "Reporte preliminar: Hacen Phishing para engañar a seguidores de Maria Corina Machado" VEsinFiltro, 27 de junio de 2024. https://vesinfiltro.org/noticias/2024-06-27-phishing-comandito/

146. "Infiltrar, robar datos, estigmatizar, atacar," Cazadores de fake news, 26 de agosto de 2024. https://www.cazadoresdefakenews.info/infiltrar-robar-datos-estigmatizar-atacar/.

147. "Hackean cuentas en Instagram de periodistas venezolanos," Espacio Público, 16 de septiembre de 2024, https://espaciopublico.ong/hackean-cuentas-en-instagram-de-periodistas-venezolanos/.

148. "ME HACKEARON MI CUENTA DE X," Prakritri Maduro (@prakritimaduro), 12 de septiembre de 2024. https://x.com/prakritimaduro/status/1834383254633509138.

149. Conversación entre el objetivo de vigilancia y Conexión Segura discutiendo medidas de seguridad digital, diciembre de 2025.

150. Entrevista a un familiar que asistió al periodista Nelson Bocaranda al intentar manejar el caso y recuperar su cuenta.

151. Entrevistas con la víctima, 2023.

152. "Redes de control: censura y represión digital en las elecciones presidenciales en Venezuela", VEsinFiltro, 26 de marzo de 2025. https://vesinfiltro.org/noticias/2025-03-12-reporte-elecciones-presidenciales/.

153. Ibid.

154. El nombre de usuario "La lista Machado" hace referencia a la Lista Tascón. Esta referencia se ha utilizado anteriormente con fines intimidatorios en otras campañas de phishing, incluida la campaña contra Voluntarios por Venezuela.

155. "Redes de control: censura y represión digital en las elecciones presidenciales en Venezuela", VEsinFiltro, 26 de marzo de 2025. https://vesinfiltro.org/noticias/2025-03-26-venezuela-represion-digital-elecciones/.

156. Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto y Sarah McKune, "Mapping FinFisher's Continuing Proliferation", [Mapear la proliferación continua de FinFisher] Citizen Lab, 15 de octubre de 2015.https://citizenlab.ca/research/mapping-finfishers-continuing-proliferación/.

157. Katherine Pennacchio, "Hacking Team casi corona en Venezuela", Armando.info, 18 de julio de 2015, https://armando.info/hacking-team-casi-corona-en-venezuela/.

158. Archivo de correo electrónico del equipo de piratería, ID de correo electrónico 359273, WikiLeaks. https://wikileaks.org/hackingteam/emails/emailid/359273.

159. Katherine Pennacchio, "Hacking Team casi corona en Venezuela", Armando.info, 18 de julio de 2015, https://armando.info/hacking-team-casi-corona-en-venezuela/.

160. Mexico, Venezuela: The small spyware providers who operate outside the limelight [Los pequeños proveedores de software espía que operan fuera del foco], Intelligence Online, 6 de enero de 2026.https://www.intelligenceonline.com/americas/2026/01/06/los-pequenos-proveedores-de-software-espia-que-operan-fuera-del-centro-de-atención,110590674-art.

161. Laura Vidal, "Desvelando la represión en Venezuela: Vigilancia y censura tras las elecciones presidenciales de julio", Electronic Frontier Foundation, 16 de septiembre de 2024. https://www.eff.org/deeplinks/2024/09/descubriendo-la-represión-en-venezuela-vigilancia-y-censura-siguiente-julios

162. "Estado de conmoción exterior en Venezuela: alcance y riesgos", Acceso a la Justicia, January 15, 2026, https://accesoalajusticia.org/estado-conmocion-exterior-venezuela-alcance-riesgos/.

163. La Constitución venezolana de 1999 protege nominalmente la inviolabilidad de las comunicaciones privadas en su artículo 48, pero esta protección ha sido sistemáticamente ignorada por las fuerzas de seguridad, especialmente durante períodos de represión política tras elecciones controvertidas. Véase "Balance #4Ago: 88 casos en medio de crisis política en Venezuela", Espacio Público, 5 de agosto de 2025. https://espaciopublico.ong/balance-4ago-88-casos-en-medio-de-crisis-politica-en-venezuela/

164. VE sin Filtro, documentación de procedimientos de control migratorio, enero de 2026.

165. "Autoridades de la UCV rechazan despliegue militar y policial durante visita de Delcy Rodríguez: «Es una violación a la autonomía»," El Pitazo, January 31, 2026, https://elpitazo.net/regiones/gran-caracas/autoridades-de-la-ucv-rechazan-despliegue-militar-y-policial-durante-visita-de-delcy-rodriguez-es-una-violacion-a-la-autonomia/.

166. La Constitución venezolana y la Ley de Universidades Nacionales garantizan la inmunidad territorial de los campus universitarios, lo que significa que policías o militares no pueden ingresar a esas zonas.

167. Oded Yaron, "Despite Sanctions, Israeli Firm Cellebrite Sold Phone-hacking Tech to Venezuela" [A pesar de las sanciones, la empresa israelí Cellebrite vendió tecnología de piratería telefónica a Venezuela], Haaretz, 10 de septiembre de 2020, https://www.haaretz.com/israel-news/tech-news/2020-09-10/ty-article/.premium/despite-sanctions-israeli-firm-sold-phone-hacking-tech-to-venezuela/0000017f-f355-df98-a5ff-f3fdba8c0000.

El Atlantic Council es una organización no partidista que promueve el liderazgo constructivo de Estados Unidos y su participación en asuntos internacionales, con base en el papel central de la comunidad atlántica para enfrentar los desafíos globales de hoy.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226
www.AtlanticCouncil.org