LOS VIGILANTES EN LA MIRA

Tecnologías de vigilancia para el control político en Venezuela

ANDRÉS AZPÚRUA • IRIA PUYOSA

Con este informe, los autores por la mediación de la organización VE SIN FILTRO nos ofrecen 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.

ABSTRACT

Through this report, facilitated by the organization VE SIN FILTRO, the authors provide a comprehensive analysis of the surveillance technologies deployed during the administration of Nicolás Maduro, which persist to this day under the tenure of acting president Delcy Rodríguez.

Apesar del cambio de liderazgo, que tuvo lugar luego de la 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.

Lo que aquí ofrecemos es un sumario ejecutivo de una investigación-informe que nos 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 del circuito cerrado de televisión –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

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.

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 en 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 explícito 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, coordinado 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.

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.

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 al 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, condicio-

nando 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.

ANDRÉS AZPÚRUA

Activista por los derechos digitales venezolano. Es el director ejecutivo de la organización Venezuela Inteligente, donde ha encabezado programas como Conexión Segura *VE Sin Filtro*. También se desempeñó como presidente del capítulo en Venezuela de *Internet Society* y como director de la Cámara Venezolana de Empresas de Tecnología de la Información.

IRIA PUYOSA

PhD de la Universidad de Michigan (2009). Formación de posgrado en investigación basada en encuestas (Universidad de Michigan) y comunicación estratégica (Universidad Católica Andrés Bello). Investigadora y consultora en comunicación política, estrategias digitales y políticas públicas para Internet. Además de investigadora senior de la Iniciativa Democracia + Tecnología del Atlantic Council.