Espionaje digital: ¿Cómo opera la vigilancia estatal en Venezuela?

TalCual

Aunque varias plataformas de mensajería instantánea ofrecen cifrado que impide el espionaje directo, el gobierno de Nicolás Maduro ha desarrollado un entramado de vigilancia sistemática a través de intervenciones telefónicas, aplicaciones estatales, monitoreo en redes sociales y herramientas forenses.

Mientras el gobierno de Nicolás Maduro insiste en que plataformas como WhatsApp son utilizadas para conspiraciones y filtrar información, la realidad apunta en otra dirección.

A pesar de su discurso público, ningún gobierno puede espiar directamente el contenido de las comunicaciones protegidas por cifrado de extremo a extremo, como el caso de WhatsApp. Sin embargo, eso no significa que la vigilancia por parte del gobierno venezolano no ocurra. Lo hace, y de forma profunda, sistemática y muchas veces ilegal, por vías alternativas.

Diversas organizaciones como IPYS Venezuela, VeSinFiltro y Freedom House han documentado cómo el régimen ha construido un aparato de control que incluye interceptaciones masivas de llamadas, aplicaciones oficiales que recolectan datos sin consentimiento, monitoreo constante de redes sociales y acceso forzado a dispositivos móviles.

Este ecosistema de vigilancia no solo pone en riesgo la privacidad individual, sino que alimenta un clima de intimidación y autocensura que erosiona la libertad digital en el país.

Dónde el gobierno de Maduro sí puede espiar

En Venezuela, el espionaje estatal no se realiza directamente a través de plataformas como WhatsApp, pero se lleva a cabo por otras vías igualmente invasivas. Entre ellas destacan:

1. Intervenciones telefónicas a gran escala

Un informe publicado en 2021 por Telefónica (empresa matriz de Movistar Venezuela) confirmó la magnitud de la vigilancia estatal. Según el reporte, más de **1,5 millones de líneas telefónicas** fueron interceptadas durante ese año, lo que equivale a casi el **20% del total de usuarios** de Movistar en el país. Estas intervenciones incluyeron la interceptación de llamadas, la supervisión de mensajes SMS, la geolocalización de personas a través de sus teléfonos móviles y el monitoreo de su tráfico de internet.

Para dimensionar el impacto de estas cifras, basta con observar el análisis comparativo incluido en el informe: **Venezuela concentró el 81% de todas las interceptaciones legales reportadas por Telefónica en los 12 países donde opera**, superando por mucho al resto de las naciones combinadas.

El hecho de que únicamente Telefónica haya publicado un informe detallando la interceptación de líneas telefónicas no significa que otras operadoras, como Digitel o Movilnet, no estén sujetas a prácticas similares. La diferencia es que estas compañías nunca han divulgado datos al respecto. Incluso en el caso de Telefónica, este tipo de información solo fue reportada una vez, lo que sugiere una falta generalizada de transparencia en el sector.

2. Aplicaciones estatales con fines de control

Aplicaciones como **VenApp**, desarrolladas bajo el paraguas del gobierno, recolectan datos personales y de geolocalización. Aunque fue presentada inicialmente como una «red social venezolana» creada por emprendedores, su verdadero propósito se ha ido revelando con el tiempo.

Originalmente diseñada para reportar fallas en servicios públicos, **VenApp fue utilizada tras las elecciones del 28 de julio de 2024 para centralizar reportes sobre protestas sociales y presuntas «Guarimbas Fascistas»**. Bajo control estatal, esta plataforma se ha convertido en una herramienta de monitoreo

ciudadano.

3. Monitoreo sistemático de redes sociales

Desde la creación del **Centro Estratégico para la Seguridad y Protección de la Patria (CESPPA)** en 2013 y la capacitación de cuerpos de seguridad —como la Guardia Nacional— en el uso de redes para «advertencias tempranas», el monitoreo digital se ha institucionalizado.

Una muestra clara es el caso de **Nelson Piñero**, militante de Encuentro Ciudadano, detenido el 21 de noviembre de 2023 por publicar comentarios críticos contra el gobierno en la red social X. Fue imputado por «incitación al odio», luego de que sus publicaciones fueran detectadas mediante «**ciberpatrullaje» del Servicio Bolivariano de Inteligencia**.

Tras las elecciones presidenciales de 2024, un informe del **Alto Comisionado de las Naciones Unidas para los Derechos Humanos** denunció que funcionarios realizaron **registros arbitrarios de teléfonos móviles** en busca de vínculos con la oposición. Además, ciudadanos reportaban a sus vecinos a través de VenApp por expresar descontento en redes sociales o grupos de WhatsApp, lo que dio lugar a operativos conocidos como la **Operación Tuntún**.

4. Uso de antenas falsas (IMSI Catchers)

Una investigación de *Armando.info* reveló la existencia de al menos **80 antenas sospechosas** en Venezuela, muchas de ellas ubicadas en zonas estratégicas de Caracas, aeropuertos y en la frontera con Colombia.

Estos dispositivos, conocidos como **IMSI Catchers** (o Stingrays/Triggerfish), simulan ser antenas de telefonía móvil para interceptar comunicaciones en un radio de hasta un kilómetro. Son portátiles, difíciles de detectar a simple vista, y pueden ocultarse en lugares tan discretos como el maletero de un vehículo o un clóset.

Una vez activados, pueden capturar llamadas, leer mensajes de texto y rastrear la ubicación exacta de un teléfono, dejando expuestos algunos datos personales sensibles.

5. Acceso forzado a teléfonos mediante herramientas forenses

Aunque no se trata de vigilancia remota, herramientas como **Cellebrite** representan otro método a través del cual las autoridades pueden acceder a la información de un teléfono. Cellebrite es un dispositivo de análisis forense que permite copiar el contenido completo de un teléfono móvil, incluso si está protegido por contraseña. Sin embargo, **solo puede ser utilizado si las fuerzas de seguridad tienen el dispositivo en su poder**, lo que usualmente ocurre tras una detención o incautación.

Esta herramienta explota vulnerabilidades en el sistema operativo o contraseñas débiles para desbloquear el dispositivo. Una vez dentro, Cellebrite extrae automáticamente fotos, registros de llamadas, historiales de ubicación, redes Wi-Fi almacenadas y, en muchos casos, el contenido de aplicaciones de mensajería o redes sociales.

Aun así, **el peligro más frecuente para la ciudadanía no son estas herramientas forenses, sino las aplicaciones espía instaladas sin consentimiento**, muchas veces bajo el disfraz de software de «control parental» o «seguridad personal». Estas apps permiten a terceros monitorear llamadas, mensajes, ubicación e incluso activar la cámara o el micrófono del teléfono sin que el usuario lo note.

6. Revisión arbitraria de teléfonos móviles

Según Andrés Azpúrua, director de VeSinFiltro, en Venezuela la vulnerabilidad de los dispositivos móviles es especialmente alta debido a prácticas abusivas por parte de cuerpos de seguridad del Estado. Una de las más extendidas es la revisión forzada de teléfonos, muchas veces sin orden judicial y bajo presión o intimidación directa.

Esta práctica ocurre en protestas, puntos de control, detenciones o simplemente durante operativos policiales en comunidades. El objetivo puede ser desde revisar redes sociales y conversaciones hasta verificar fotos, contactos o aplicaciones instaladas. Aunque no siempre se utilizan herramientas forenses como Cellebrite, el acceso físico al dispositivo es suficiente para exponer información personal sensible y generar nuevas formas de persecución.

Más allá de WhatsApp: ¿cómo resguardar tu seguridad digital en Venezuela?

En un contexto donde el monitoreo estatal se ha vuelto sistemático y agresivo, es fundamental adoptar medidas de autoprotección digital. A continuación, algunas recomendaciones clave para proteger tu privacidad y seguridad en Venezuela:

1. Usa aplicaciones con cifrado de extremo a extremo

Para comunicarte de forma segura, es crucial utilizar **aplicaciones de mensajería que ofrecen cifrado de extremo a extremo**. Esto significa que solo tú y la persona con la que estás hablando pueden leer los mensajes o escuchar las llamadas. Las más recomendadas son:

- **Signal**: Considerada una de las apps más seguras. No solo cifra mensajes y llamadas, sino que también permite participar en grupos sin necesidad de mostrar tu número de teléfono. Puedes usar un alias y proteger tu identidad.
- **WhatsApp**: También ofrece cifrado de extremo a extremo, aunque comparte ciertos metadatos con su empresa matriz (Meta), por lo que no es tan privada como Signal.

Importante: **Evita las llamadas tradicionales o mensajes SMS**, ya que son fácilmente interceptables y no están cifrados.

2. No descargues aplicaciones del gobierno

Apps como **VenApp** han sido señaladas por recolectar datos personales, acceso a contactos, ubicación en tiempo real y contenido publicado en redes sociales. Descargarlas representa un riesgo directo a tu privacidad, especialmente si estás vinculado a actividades críticas del gobierno o eres parte de la oposición.

3. Cuidado con lo que publicas en estados y grupos

Aunque plataformas como WhatsApp ofrecen cifrado, **los estados y mensajes en grupos se comparten con varias personas**, lo que aumenta el riesgo de filtraciones. Incluso si confías en tus contactos, recuerda que **los teléfonos pueden ser inspeccionados durante detenciones y allanamientos**, como ya ha ocurrido en Venezuela.

Evita compartir contenido sensible o que pueda usarse en tu contra, publicar ubicaciones o detalles personales en estados y formar parte de grupos grandes o desconocidos.

4. Para activistas, periodistas y defensores de derechos humanos: prioriza Signal

A diferencia de otras aplicaciones, Signal permite crear grupos sin necesidad de compartir tu número telefónico, lo que ofrece una capa adicional de anonimato y seguridad. Además, **puedes configurar un alias en lugar de usar tu nombre real, lo cual resulta clave si el objetivo es mantener protegida tu identidad y la de tus contactos**. En caso de que tu teléfono sea incautado o revisado por autoridades, esta característica puede evitar que se revelen conexiones personales o profesionales sensibles.

Signal también incluye funciones de seguridad avanzadas como **mensajes que se autodestruyen, protección por PIN y la posibilidad de establecer bloqueos adicionales a la aplicación**. Incluso, permite cambiar el ícono y el nombre de la app en el dispositivo, para que no pueda ser identificada fácilmente en una inspección visual.

Estas medidas convierten a Signal en una herramienta de comunicación especialmente diseñada para operar en contextos de riesgo, como el que enfrentan quienes documentan abusos o participan en la defensa de derechos humanos en Venezuela.

5. Cuidado con descargas y enlaces desconocidos

Muchas veces el riesgo no está solo en los enlaces que circulan por WhatsApp, sino en prácticas cotidianas como descargar videojuegos, instalar programas «crackeados» o hacer clic en enlaces que llegan sin verificación previa. Estas acciones pueden instalar malware o spyware sin que el usuario lo note, comprometiendo seriamente la seguridad del dispositivo y la privacidad de quien lo usa.

Adrián González, director de la ONG Cazadores de Fake News, advierte que «a veces se cree que el riesgo está en los enlaces de WhatsApp porque se dice que contienen virus, pero en realidad muchos son intentos de phishing. En todo caso, siempre hay que evitar hacer clic en enlaces y ejecutar programas si no se tiene certeza de quién los envió o de su origen».

6. Usa dispositivos que reciban actualizaciones de seguridad

Andrés Azpúrua, director de VeSinFiltro, advierte que **una parte importante de los teléfonos usados en Venezuela ya no recibe actualizaciones de seguridad del sistema operativo**, lo que deja abiertas fallas conocidas y aumenta el riesgo de vigilancia o infección por software malicioso.

Para protegerte, **usa dispositivos que garanticen actualizaciones periódicas durante todo el tiempo que planeas tenerlos**. Marcas como **Samsung** y **Google Pixel** ofrecen políticas claras de soporte por varios años desde el lanzamiento del modelo. **Apple**, aunque no publica cifras oficiales, suele liderar en duración de soporte.

Sembrar el miedo, una estrategia para censurar

Más allá de los aspectos técnicos o legales, las acusaciones del gobierno de Nicolás Maduro contra WhatsApp deben entenderse en **un contexto de control político de la información**. En Venezuela, la libre circulación de mensajes por canales no controlados por el Estado representa una amenaza directa para un gobierno que basa parte de su poder en el dominio de la narrativa pública.

En ese sentido, crear rumores y desinformación sobre supuestos espionajes, bases de datos filtradas o conspiraciones extranjeras cumple una función estratégica: infundir temor, desalentar el uso de una plataforma que el gobierno no puede vigilar de manera constante.

Pero la campaña de descrédito contra WhatsApp no solo busca silenciar una vía de comunicación libre. También prepara el terreno para justificar la creación de una aplicación nacional, similar en funciones, pero controlada por el gobierno, como ya ha ocurrido en países aliados como Rusia (con su red *Gosuslugi*) o China (con plataformas como WeChat, altamente vigiladas). La mención de un «sistema de mensajería propio y seguro» por parte de Maduro, sumada a experiencias como VenApp, que ya permite el rastreo de ubicación y el cruce de datos personales, apuntan en esa dirección.

Como advierte el experto en seguridad digital, David Aragort, **la experiencia venezolana demuestra que imponer nuevas plataformas estatales ha sido históricamente un fracaso**. «Desde hace muchos años, incluso desde la época de Chávez, se han intentado lanzar herramientas propias, y todas han fracasado en mayor o menor medida. No creo que sea viable en el mediano plazo, incluso si restringen el acceso a todas las demás redes sociales», señala.

En esa línea, Adrián González, director de la ONG Cazadores de Fake News, apunta a que está claro que una aplicación que esté bajo control de un gobierno, sea cual sea, representa intrínsecamente un problema de seguridad para el usuario.

«Si hoy en día los gobiernos deben hacer acuerdos con plataformas como WhatsApp o Telegram para acceder a ciertos datos —y aun así no pueden obtener el contenido de los mensajes por el cifrado—, imagina el riesgo que supondría que ese control estuviera completamente en manos del Estado. Sería un problema de seguridad muy grave para los ciudadanos y dudo mucho que la gente quiera instalar y usar una app sabiendo que el gobierno podría tener acceso directo a sus contactos, ubicación, horarios de conexión y otras formas de información sensible».

Para Valentina Aguana, activista por los derechos digitales, **toda aplicación desarrollada o respaldada por el gobierno venezolano representa un riesgo para la seguridad digital de la ciudadanía**. No obstante, aclara que el principal obstáculo para el régimen no es el desarrollo tecnológico, sino la adopción masiva.

«Mientras no existan bloqueos o restricciones activas contra las plataformas más usadas, es poco probable que una app oficial impuesta desde el poder pueda desplazar a las ya consolidadas».

A pesar de lo que digan, lo que el gobierno de Maduro se plantea no es precisamente proteger a la población del «espionaje extranjero», sino centralizar las comunicaciones digitales bajo una herramienta estatal, desde la cual sí se pueda tener acceso a conversaciones, ubicaciones, relaciones sociales y patrones de comportamiento político.

Es una estrategia que combina miedo, difamación, propaganda y sustitución tecnológica con fines de vigilancia, y representa un nuevo frente de disputa en la lucha por la libertad de expresión en Venezuela.

https://talcualdigital.com/espionaje-digital-como-opera-la-vigilancia-estatal-en-venezuela/