

Espionaje digital masivo en Venezuela: ¿cómo funciona y cómo protegerse?

El experto en seguridad digital Andrés Azpúrua desveló la preocupante realidad del espionaje digital en Venezuela. La entrevista analizó cómo opera [la vigilancia estatal](#) y cómo los ciudadanos pueden protegerse. Azpúrua, fundador de la organización Conexión Segura y Libre (VeSinFiltro), proporcionó datos contundentes y recomendaciones prácticas para navegar este complejo panorama.

Uno de los puntos más alarmantes fue la evidencia de «intervenciones telefónicas a gran escala». Azpúrua se refirió a [un informe de Telefónica \(2021\)](#) que «habla de dos tipos de datos: la interceptación de las comunicaciones (contenido de llamadas, mensajes de texto, tráfico de internet y ubicación del teléfono) y los metadatos (información sobre la comunicación, como la lista de personas contactadas y la duración de las llamadas)». El informe revela que en Venezuela «básicamente, digamos, cualquiera puede pedir esa información», a diferencia de otros países donde existe un mayor control judicial. Venezuela concentra el 81% de las interceptaciones legales reportadas por Telefónica en 12 países, un dato que, según el experto, «muestra una realidad un poco más completa».

El crecimiento de las solicitudes de interceptación entre 2018 y 2021 es significativo, representando más del 20% de las líneas de suscriptores en Venezuela, en comparación con porcentajes inferiores al 0,1% en otros países donde opera Telefónica. Azpúrua enfatizó que aunque esto no significa que «para cada llamada... hay alguien escuchándolo en tiempo real», sí indica una vigilancia masiva. Además, se planteó la preocupación de que otras empresas de telecomunicaciones venezolanas, como Movilnet y Digitel, puedan estar realizando prácticas similares.

La entrevista también abordó el uso de aplicaciones estatales para la vigilancia, específicamente la aplicación VenApp. Azpúrua explicó que esta aplicación, inicialmente ofrecida en las tiendas de aplicaciones de Apple y Google, [fue retirada debido a preocupaciones de seguridad y transparencia](#). Sin embargo, sigue disponible para descarga directa desde internet o a través del sistema Patria. Azpúrua destacó [el uso de VenApp para «sapear a personas](#) por estar en descontento con el gobierno», un uso que «rebasaba todos los límites» de las

políticas de las tiendas de aplicaciones.

Otro aspecto crucial fue el «monitoreo sistemático de redes sociales». Azpúrua señaló que este monitoreo, institucionalizado desde la creación del [Cesppa](#) en 2013, implica «funcionarios públicos metiéndose en Twitter, metiéndose en redes sociales, viendo lo que la gente comenta, lo que la gente publica». Este monitoreo se utiliza para identificar personas para su detención o para aumentar la vigilancia, incluso recibiendo denuncias de otros usuarios. Este tipo de prácticas fueron mencionadas en [un informe de la ONU sobre la situación de derechos humanos en Venezuela](#), donde se documentaron «registros arbitrarios de teléfonos móviles en busca de vínculos con la oposición». Azpúrua enfatizó la gravedad de estas acciones, completamente ilegales y sin apego al derecho.

La entrevista también tocó el tema del uso de antenas falsas (IMSI catchers), [citando el proyecto FADE](#), que detectó irregularidades en 33 torres celulares en Caracas en 2019. Azpúrua explicó que los IMSI catchers son «antenas falsas que monta un tercero haciéndose pasar por las antenas de una empresa», permitiendo el acceso al contenido de las llamadas, mensajes de texto y la ubicación de los usuarios. La ubicación estratégica de estas antenas permite un monitoreo directo de conversaciones y actividades en zonas específicas.

Finalmente, se discutió el uso de herramientas como Cellebrite, un dispositivo que permite extraer datos de teléfonos celulares con acceso físico. Azpúrua confirmó la presencia de este tipo de equipos en Venezuela, utilizados para «extraer toda la información, fotos, ubicación, aplicaciones, contenido de chats», pero cuando se tiene acceso físico al dispositivo, no a distancia. Aunque diseñadas para investigaciones criminales, en Venezuela se abusa de estas herramientas.

Recomendaciones para reforzar la privacidad digital:

- * **WhatsApp:** Utilizar la opción de «mensajes secretos», activar la verificación en dos pasos, configurar el borrado automático de mensajes y tener un PIN fuerte.
- * **Signal:** Considerar el uso de Signal como una alternativa más segura que WhatsApp, aplicando las mismas medidas de seguridad mencionadas anteriormente. Ocultar la aplicación para mayor discreción.
- * **Actualizaciones:** Mantener actualizados el sistema operativo

del teléfono y las aplicaciones para mejorar la seguridad.

* **Descargas:** Evitar descargar aplicaciones de fuentes desconocidas fuera de las tiendas oficiales de aplicaciones (App Store y Google Play).

* **PIN fuerte:** Utilizar un PIN alfanumérico complejo para proteger el acceso al teléfono.

La privacidad en las comunicaciones está garantizada en el artículo 48 de la [Constitución venezolana vigente](#), que reza: «Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso».

Con información de TalCual