ALERTA SPYWARE

Vía Libre

DEMOCRACIA EN RED

O.D.I.A.

CELS

newventurefund

El riesgo del software espía en la Argentina

MAYO 2026

Índice

INTRODUCCIÓN

El *spyware* (software espía) es un tipo de software malicioso que interfiere en el funcionamiento normal de un dispositivo (computadora, tablet, teléfono móvil) para recopilar información sin alertar a la persona usuaria y después la envía a otra entidad no autorizada. Esto quiere decir que funciona de manera subrepticia y, muchas veces, ilícita.

Su uso se ha incrementado en los últimos años a partir de la expansión de la encriptación de comunicaciones. Hoy en día, la mejor forma de conocer el contenido de una comunicación no es interceptarla, sino espiarla en su punto de inicio o final, es decir, en los dispositivos. Esto transforma al *spyware* en una herramienta de investigación... pero también, con preocupante frecuencia, de espionaje ilegal.

Así, mientras algunos actores (fabricantes, gobiernos, fuerzas de seguridad, agencias de inteligencia, funcionarios judiciales) ponderan sus virtudes y sobre todo su necesidad, al mismo tiempo el *spyware* demostró ser una amenaza de primer orden para la privacidad y los derechos humanos.

Representa un riesgo enorme por su profunda capacidad invasiva y de acceso indiscriminado a información personal y sensible, que además sigue operando sin que la víctima lo note. Su uso ilegal implica una forma de ataque dirigido, distinto de otras formas de vigilancia que son masivas. Por ello, las personas que están más en riesgo son aquellas que por distintas razones están políticamente expuestas: opositores o disidentes políticos, legisladores, periodistas, activistas[1].

Las empresas y gobiernos afirman que el uso del *spyware* se limita a delitos graves, como terrorismo o criminalidad organizada. Sin embargo, la cantidad de casos de uso ilegal de esta herramienta en países tan diversos como Arabia Saudita, Italia o Estados Unidos, y en nuestra región México, El Salvador, Perú o Colombia, muestran que una vez que estas herramientas son adquiridas por los Estados resulta muy difícil evitar su despliegue en prácticas de inteligencia ilegal, aún en países con una institucionalidad sólida. Por ello algunas organizaciones de la sociedad civil sostienen la necesidad de aplicar una “moratoria”, es decir, una prohibición temporal de uso de estas herramientas hasta que se puedan desarrollar

salvaguardas que anulen o minimicen los riesgos asociados a ellas[2].

En la Argentina, si bien existen rumores nunca confirmados sobre su circulación local, hasta el momento no se registraron casos de uso legal ni ilegal de *spyware*. Pero al mismo tiempo, una serie de factores estructurales y coyunturales elevan el nivel de riesgo de que la utilización ilegal del *spyware* se difunda en la Argentina.

Este documento parte entonces de la base de que aún estamos a tiempo de evitar las peores consecuencias y de desarrollar instrumentos y políticas de control. Pero también busca alertar sobre las debilidades que nos ponen en un peligro real de pasar a engrosar la lista de países donde el *spyware* se utiliza para la persecución política y la vulneración de derechos básicos.

Presentamos los 7 principales factores de riesgo que identificamos en nuestro país, con el objetivo de proponer acciones preventivas que puedan fortalecer capacidades del Estado y la sociedad civil para controlar el uso de estas tecnologías sumamente invasivas.

---

1 Existe una lista actualizable de víctimas del software Pegasus, desarrollado por la firma israelí NSO. Se trata de una herramienta tipo *spyware* que estuvo involucrada en escándalos en más de 50 países. Al menos 180 periodistas fueron espiados de manera ilegal con este software. La lista permite hacerse una idea del perfil de personas en riesgo de ser espiadas de manera ilegal a través de *spyware:* https://github.com/GranittHQ/data-pegasus-victims/blob/main/data-pegasus-victims.csv

2 Amnesty International, "Towards a Global Moratorium on Targeted Surveillance Technology", 2022. Disponible en: *https://www.amnesty.org/en/wp-content/uploads/2022/11/POL4061542022ENGLISH.pdf*

Un País Federal con Regulaciones Débiles y Ambiguas

UN PAÍS FEDERAL CON REGULACIONES DÉBILES Y AMBIGUAS

Hasta marzo de 2026, 9 jurisdicciones habían incorporado regulación que habilitaría el uso de *spyware*, mientras que otras 15 poseen normativas que, dado su carácter vago e impreciso, podrían habilitarlo siguiendo una interpretación amplia de su código de forma. Estos procesos de incorporación normativa no responden a un diseño integral orientado a la protección de derechos fundamentales, sino que cada provincia avanza de manera autónoma. El resultado es un mosaico de soluciones disímiles y carentes de salvaguardas estrictas, que multiplica las instancias decisorias y amenaza con generar contradicciones normativas.

En numerosos casos, el *spyware* es incorporado mediante su simple asimilación a categorías preexistentes, sin el desarrollo de figuras específicas que contemplen su complejidad técnica. En otros, aun cuando se lo reconoce como una herramienta de investigación diferenciada, su regulación se introduce sin la adopción de estándares estrictos, por lo que no se tiene en cuenta su naturaleza riesgosa.

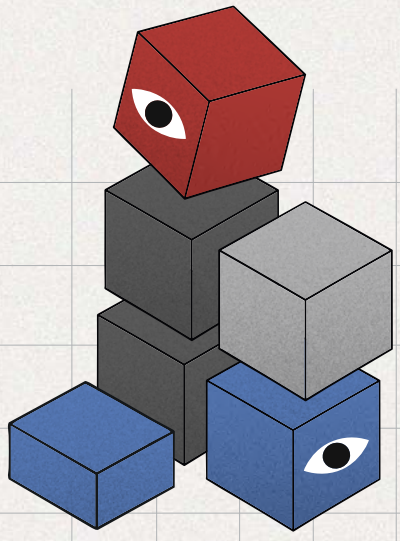
La legislación existente no define las hipótesis de investigación que habilitan el uso de herramientas de *spyware*. Se recurre con frecuencia a fórmulas amplias —como la "interceptación de comunicaciones", las denominadas "medidas de investigación tecnológica" o figuras como el "allanamiento remoto"— que no distinguen adecuadamente entre técnicas de investigación acotadas y mecanismos que permiten el acceso indiscriminado a dispositivos personales. No se prevén cuestiones básicas como la necesidad de precisar el tipo de información a recabar, la limitación funcional de la medida y la prohibición expresa de prácticas de vigilancia exploratoria o indiscriminada, orientadas a evitar dinámicas de "pesca de prueba".

A esto se suma que la normativa en general no establece límites temporales estrictos para el uso de la herramienta. No se establecen plazos máximos claramente definidos para la duración de estas medidas, ni criterios exigentes para su prórroga, ni mecanismos de caducidad automática una vez alcanzados los objetivos de la investigación.

Sin estas especificaciones, la normativa tiende a diluir el carácter excepcional

de una medida tan invasiva, debilita los controles y refuerza la discrecionalidad judicial.

Esta indeterminación temporal refuerza la discrecionalidad judicial y debilita los controles sobre medidas que, por su naturaleza, deberían encontrarse sujetas a estándares reforzados de necesidad y proporcionalidad.



Federalismo Policial y Multiplicación de Agencias

FEDERALISMO POLICIAL Y MULTIPLICACIÓN DE AGENCIAS

Los desafíos que implica la organización federal del país a la hora de controlar herramientas muy invasivas como el *spyware* no se limita a la fragmentación de la normativa. Los riesgos se ven particularmente acentuados por la existencia de un federalismo policial que multiplica las fuerzas de seguridad con autonomía operativa, administrativa y presupuestaria a nivel provincial y local.

A diferencia de otros instrumentos de investigación de uso puntual, el *spyware* constituye una capacidad tecnológica permanente. El mero hecho de poseerla amplía de manera significativa el riesgo institucional asociado a la vigilancia estatal.

Las policías provinciales y fuerzas locales se encuentran orientadas a la investigación y prevención de delitos ordinarios, en el marco del funcionamiento cotidiano del sistema penal. La eventual habilitación del acceso a herramientas de *spyware* para estas agencias implica que tecnologías de vigilancia de extrema intrusividad puedan integrarse a prácticas regulares de investigación criminal, desdibujando el carácter excepcional con el que se las debería utilizar. La normalización del acceso de múltiples agencias en todo el país a este tipo de herramientas aumenta exponencialmente el riesgo de su uso ilegal.

Además, esto implica la multiplicación de actores habilitados para la contratación de software de vigilancia extrema, lo que torna materialmente inviable la implementación de una metodología de contratación pública uniforme que incorpore salvaguardas comunes en materia de derechos humanos, protección de datos personales, transparencia y rendición de cuentas. Como resultado, distintas fuerzas podrían acceder a herramientas de *spyware* a través de proveedores diversos, bajo contratos heterogéneos y con cláusulas que varían sustancialmente en aspectos críticos como los límites de uso, obligaciones de auditoría y mecanismos de supervisión. La fragmentación del acceso no solo incrementa la probabilidad de usos desproporcionados, sino que también debilita la posibilidad de atribuir responsabilidades claras frente a eventuales irregularidades.

Un Estado Opaco y con Débiles Controles

UN ESTADO OPACO Y CON DÉBILES CONTROLES

Las capacidades de control de los diferentes poderes del Estado y de la sociedad civil sobre los asuntos vinculados a la seguridad, la investigación criminal, la inteligencia y la defensa siempre fueron débiles en la Argentina. En los últimos años esta característica se ha acentuado: es cada vez más difícil que policías, espías, funcionarios y judiciales rindan cuentas de lo que hacen. Con este panorama, los riesgos de que, una vez adquiridas, las herramientas tipo *spyware* sean utilizadas sin supervisión y de manera ilegal son enormes.

Las actividades estatales deberían poder ser controladas públicamente, especialmente cuando suponen un nivel de intrusión alto en la vida privada de los y las ciudadanas. En sentido contrario, el marco normativo que regula este tipo de actividad en Argentina habilita un alto nivel de secreto, generalmente bajo el paraguas vago y amplio de la "seguridad nacional".

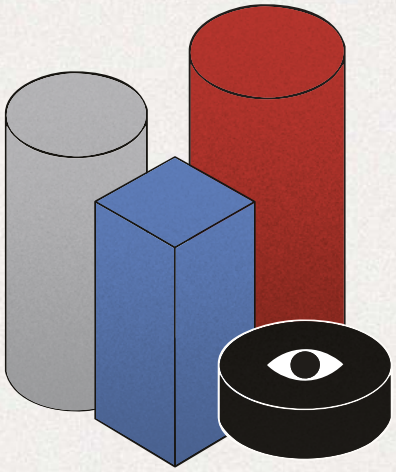
Es el caso, por ejemplo, de la Ley de Inteligencia y sus modificaciones, que prevén excepciones muy amplias al control público. Estas excepciones se volvieron la regla a través del DNU 941/25, que declara como "encubierta" cualquier actividad realizada por organismos que componen el Sistema de Inteligencia Nacional. Esto incluye también a dependencias de las fuerzas de seguridad que despliegan tareas de este tipo. El nivel de opacidad con el que operan es incompatible con los estándares internacionales de transparencia en democracia.

Algo similar sucede con la propia ley de Acceso a la Información Pública y su reglamentación (modificada por decreto en 2024), que contiene también algunos supuestos vagos que habilitan a los organismos a evitar fácilmente la entrega de información.

Además, al incorporar el uso de tecnologías para estas actividades, aparece también la salvaguarda legal del "secreto comercial", derivado de regulaciones de propiedad intelectual, para evitar informar de qué manera y con qué parámetros funcionan esos sistemas. Tal fue el caso del software utilizado por la CABA para el reconocimiento facial de prófugos, donde sigue

pendiente la auditoría a la tecnología porque la empresa no entregó el código fuente ni los data sets. Se trata de un sistema de licencias de software de uso privativo, contratado “a caja negra”, donde el Gobierno nunca supo cómo funciona, bajo qué parámetros fue entrenado y bajo qué criterio arriba a resultados.

Este escenario resulta aún más crítico en países que, como la Argentina, presentan una historia persistente de violencia institucional y déficits estructurales en los mecanismos de control público y rendición de cuentas sobre las fuerzas de seguridad. Muchas fuerzas policiales siguen funcionando con el modelo de “asuntos internos”, es decir, se investigan a sí mismas. Y son pocos los casos de las auditorías externas con capacidad y voluntad política de ejercer un control efectivo sobre las policías.



Malos Antecedentes: la Tecnología se Incorpora de Manera Express

MALOS ANTECEDENTES: LA TECNOLOGÍA SE INCORPORA DE MANERA EXPRESS

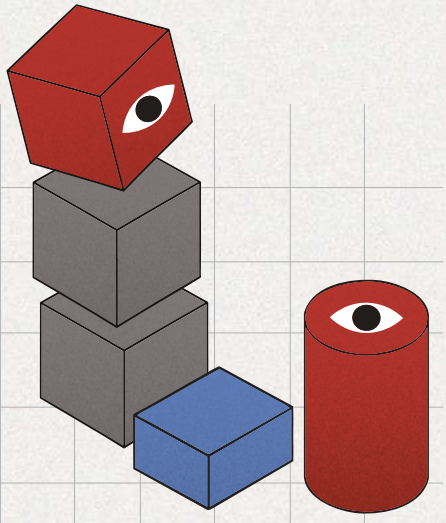
La experiencia de los últimos años en Argentina muestra que la tecnología para vigilancia se incorpora sin regulación, sin debates, sin evaluaciones de impacto ni de performance.

Bajo pretextos de “modernización” y de eficientización de las políticas de seguridad, el Estado argentino adopta cada vez más tecnologías de manera indiscriminada. La urgencia y gravedad de las “nuevas amenazas”, como el narcotráfico y el terrorismo, parecen alcanzar como justificación para la implementación de dispositivos de vigilancia de manera rápida, unilateral (esquivando el Congreso), sin información pública disponible y sin ninguna evaluación sobre el impacto en derechos, como si fueran excluyentes. Como ya se dijo, el control ciudadano es muy débil, y el conocimiento sobre su funcionamiento también es escaso desde el propio Estado. Si la incorporación del *spyware* se realiza según los patrones que caracterizaron a otras tecnologías de vigilancia (cámaras de seguridad, reconocimiento facial, inteligencia artificial), el uso abusivo es una posibilidad cierta.

No hay aún normativa específica que rija el procedimiento para la incorporación de tecnologías invasivas por parte del Estado. Algunas leyes permiten establecer ciertos límites y salvaguardas: la ley de Protección de Datos Personales, de Acceso a la Información Pública, de Inteligencia Nacional, de Seguridad Interior, según los usos de esas tecnologías. Sin embargo, se trata de un marco normativo desactualizado e insuficiente en este sentido que, por ejemplo, no exige evaluaciones previas de impactos en derechos que midan los riesgos y la efectividad real, pruebas de *performance*, tasas de error y/o sesgos, auditabilidad, consultas públicas de forma previa al despliegue ni estándares de control luego. Adquirir e implementar softwares de vigilancia sin una evaluación de impacto previa impide obtener una valoración anticipada de los efectos adversos que podría tener, como vulneraciones, sesgos e impactos diferenciados, y en muchos casos el daño posterior es irreparable. Al mismo tiempo, la falta de consulta pública previa a los procesos de licitación y contratación de tecnologías de vigilancia se traduce en una erosión de la legitimidad democrática, en tanto

no se propicia un debate informado sobre la idoneidad y los límites éticos de estas herramientas.

Este marco normativo, junto con la narrativa que promueve la incorporación de tecnologías como un evento positivo per se, llevó a un despliegue importante de softwares de distinto tipo para el control y la seguridad nacional, así como para la función judicial. En ningún caso se realizaron, al menos de manera pública, evaluaciones de impacto ni tests de razonabilidad, proporcionalidad y necesidad.



Más Antecedentes Malos: descontrol en el Uso de Herramientas de Vigilancia

MÁS ANTECEDENTES MALOS: DESCONTROL EN EL USO DE HERRAMIENTAS DE VIGILANCIA

Una derivación de la debilidad estructural en el control de las fuerzas de seguridad y servicios de inteligencia es la multiplicación de casos en los que los recursos de estas agencias son "desviados" para usos ilegales. Ya sea con fines como espiar u hostigar a familiares, pasando por la extorsión económica, hasta vigilancia política ilegal, cada vez que se conoce un caso de este tipo, se señala que se trata de grupos "díscolos". Se trata de verdaderas "pymes" que utilizan estas herramientas para fines particulares, escapando supuestamente al encuadre y el control institucional. La reiteración de este tipo de casos en las últimas décadas no augura nada bueno de cara a la posible adopción de herramientas de *spyware* por parte de distintas agencias.

Este problema se agudiza porque las policías y los servicios de inteligencia se componen en general de estructuras con autonomía operativa, en las que las decisiones relativas al uso de estas herramientas se adoptan de manera fragmentada, sin un centro único de coordinación ni criterios homogéneos de aplicación. En este contexto, la definición de cómo, cuándo y con qué alcances se emplean estas capacidades queda librada a prácticas administrativas internas, sin un marco operativo robusto que permita garantizar un uso conforme a derecho, y facilitando el abuso.

La ausencia de mecanismos técnicos efectivos de control constituye uno de los principales factores de riesgo asociados al uso de *spyware*. La falta de registros de actividad completos y auditables (logs), de sistemas estrictos de gestión de permisos, de separación funcional de roles y de auditorías externas e independientes impide garantizar la trazabilidad de las operaciones realizadas. Sin estos instrumentos, resulta materialmente difícil reconstruir de manera fiable quién utilizó el sistema, en qué momento, con qué alcance y bajo qué justificación concreta, debilitando los esquemas de supervisión y dificultando la atribución de responsabilidades ante eventuales irregularidades.

La combinación de alta capacidad intrusiva y bajo nivel de control técnico

genera un entorno especialmente propicio para el desvío del uso normal de las herramientas de *spyware*. En tales escenarios, la herramienta deja de operar como un recurso excepcional al servicio del interés público y pasa a constituir una capacidad susceptible de apropiación informal en términos funcionales, integrada a dinámicas organizacionales opacas y de difícil control, cuando no directamente criminales.

La Debilidad del Estado Frente a las Empresas

LA DEBILIDAD DEL ESTADO FRENTE A LAS EMPRESAS

Además de las limitaciones existentes para controlar el accionar de las agencias estatales, la incorporación de tecnologías de vigilancia introduce un problema adicional vinculado a las condiciones en las que el Estado adquiere estas herramientas. Los procesos de contratación pública en este ámbito son poco transparentes y se realizan bajo marcos normativos poco específicos, lo que dificulta el control externo por parte de otros poderes del Estado y de la sociedad civil. Esta situación resulta especialmente problemática cuando se trata de tecnologías altamente intrusivas, cuyo funcionamiento no es fácilmente verificable y que, por su propia naturaleza, tienen capacidad de daño.

A esto se suma una marcada asimetría entre el Estado y las empresas proveedoras. Mientras estas últimas cuentan con un conocimiento técnico profundo sobre los productos que desarrollan y comercializan, los organismos estatales carecen en muchos casos de capacidades suficientes para evaluar adecuadamente qué están adquiriendo. En la práctica, esto se traduce en la compra de sistemas que operan como “cajas negras”, sin acceso al código fuente, sin posibilidades de auditoría independiente y sin garantías claras sobre sus límites de funcionamiento.

Esta asimetría no sólo afecta la instancia de adquisición, sino que se prolonga a la implementación y uso. La falta de transferencia de conocimientos y capacidades técnicas dentro del Estado genera una dependencia sostenida respecto de los proveedores, que pueden terminar condicionando tanto la operación como la supervisión de las herramientas adquiridas. A ello se suma que, en muchos casos, los procesos de adquisición tienden a privilegiar soluciones de rápida implementación y fácil utilización por parte de las fuerzas de seguridad, por sobre sistemas que incorporen mayores garantías de auditabilidad, transparencia o control.

En conjunto, estas condiciones configuran un escenario en el que la incorporación de spyware no sólo amplía las capacidades de vigilancia estatal, sino que lo hace sobre una base institucional frágil, atravesada por opacidad en las compras, dependencia tecnológica, fragmentación federal y limitaciones estructurales de control. Mientras que por un lado se incrementa la supuesta capacidad operativa de las fuerzas, por el otro se erosionan las capacidades de control sobre las mismas.

Una Coyuntura Política Propicia para la Vigilancia Masiva y la Inteligencia Ilegal

UNA COYUNTURA POLÍTICA PROPICIA PARA LA VIGILANCIA MASIVA Y LA INTELIGENCIA ILEGAL

Para alertar sobre los riesgos del uso de *spyware* para vulnerar derechos en la Argentina no sólo hay que tener en cuenta las debilidades estructurales que caracterizan nuestra relación con las tecnologías de vigilancia, sino una coyuntura política que es especialmente propicia para el desarrollo de prácticas de vigilancia masiva e inteligencia ilegal, configurando una especie de tormenta perfecta para el abuso de herramientas de software espías.

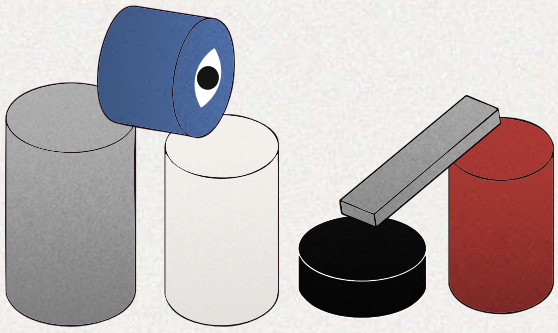
El gobierno argentino asumido en diciembre de 2023 suma una serie de características que aumentan estos riesgos. A nivel internacional, se optó por un alineamiento automático y sobreactuado con todas las decisiones que toman Estados Unidos e Israel en términos geopolíticos, de defensa y de vigilancia interna. Se trata de dos países que promueven estándares especialmente bajos de control sobre este tipo de tecnologías, a diferencia por ejemplo de los mejores estándares europeos. También abogan por la ampliación de la excusa de "seguridad nacional" para evitar cualquier tipo de rendición de cuentas. La campaña de demolición del derecho internacional que vienen protagonizando, a la que se suma la Argentina de manera voluntaria y entusiasta, es correlativa de los usos intensivos de las tecnologías para vigilar, espiar y atacar tanto blancos militares como población civil. Los países de la región subordinados a esta estrategia (Argentina, El Salvador, Ecuador, entre otros) reproducen estas decisiones a escala interna y salvando las distancias en cuanto a capacidades.

A nivel interno, el gobierno avanzó con dos reformas por decreto del sistema de inteligencia que aumentan los niveles de secreto y opacidad y amplían las atribuciones de los espías. Se conocieron además los planes estratégicos del sistema de inteligencia, que señala blancos para la vigilancia (o "riesgos") manifiestamente ilegales en términos de la Ley de Inteligencia Nacional, y que implican espiar tanto a periodistas y opositores, como a movimientos sociales, grupos ambientalistas y comunidades indígenas. Las policías también ampliaron sus atribuciones de vigilancia e inteligencia, y vienen incorporando sin ningún tipo de control herramientas tecnológicas para hacerlo. El poder judicial aún no dio respuestas sobre estas situaciones.

Se trata además de un gobierno que, directa o indirectamente, tiene muy

buenas relaciones con las empresas nacionales y extranjeras relacionadas a la industria de la seguridad y la defensa, con fuertes incentivos políticos y económicos para incorporar todo tipo de tecnología de vigilancia y espionaje. Esto hay que leerlo en el contexto de la debilidad histórica y estructural del Estado argentino para poner condiciones a este tipo de empresas.

Atravesamos entonces una coyuntura política que no hace más que exacerbar todos los riesgos que hemos descripto en los puntos anteriores.



QUÉ HACER

El diagnóstico central que sustenta estas recomendaciones enfatiza que el *spyware* es una herramienta altamente intrusiva, cuyo uso debería estar fuertemente regulado y limitado. En la Argentina, las debilidades del control de las fuerzas de seguridad y los sistemas de inteligencia, y la fragmentación de las normas, conspiran contra ello. La adquisición, la habilitación judicial y la ejecución operativa de estas herramientas se rigen por estándares desarticulados entre sí, lo que acaba por generar esquemas de control ineficaces. En este sentido, debe abandonarse el enfoque por etapas y se deben adoptar marcos normativos que contemplen el ciclo completo de vida de la herramienta, que va desde su adquisición inicial hasta la destrucción o archivo de la información obtenida.

- Esto supone que las condiciones establecidas en la contratación pública sean compatibles con los estándares de habilitación procesal y con los protocolos de ejecución, y que ninguna etapa pueda operar con independencia de las restantes.

- Las autoridades competentes en materia de contratación pública deben incorporar, en los pliegos y procedimientos de adquisición de este tipo de herramientas, requisitos técnicos mínimos referidos al alcance funcional, las capacidades de configuración y los mecanismos de registro de actividad. Estos estándares (como piso mínimo y sin ánimo de ser taxativos), deben ser definidos con participación de organismos técnicos independientes y resultar compatibles con las exigencias de proporcionalidad y razonabilidad que rigen la habilitación judicial.

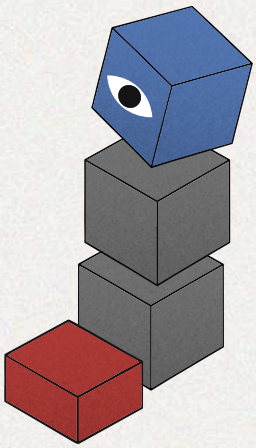
- Los marcos procesales habilitantes de estas técnicas especiales de investigación hoy se limitan a regular el momento de la autorización judicial sin incorporar mecanismos de supervisión efectiva y continua durante la ejecución de la medida, ni tampoco remedios posteriores o mecanismos de control ulterior. En particular, este derecho de forma debe prever: (a) la obligación de informar al juez interviniente sobre los métodos y alcances técnicos de la herramienta utilizada; (b) la actualización de la autorización ante cualquier modificación sustancial en el modo de ejecución; y (c) instancias de revisión judicial una vez concluida la intervención, orientadas tanto a verificar la proporcionalidad de lo efectivamente ejecutado respecto de lo autorizado, como para obtener medidas tendientes a la reparación de un potencial daño.

- Se recomienda establecer, como condición de validez del uso del *spyware*, la existencia de registros técnicos y documentales que permitan reconstruir el ciclo completo de implementación. Esta trazabilidad completa implica saber qué herramienta fue utilizada, con qué configuración, en qué momento, sobre qué dispositivos y con qué resultados. Estos registros deben ser generados de manera automática, resguardados bajo condiciones de integridad verificable y estar disponibles para la supervisión judicial y los órganos de control independiente. La trazabilidad no es una exigencia burocrática adicional, sino que en este caso constituye la condición técnica que hace posible su compatibilidad con el andamiaje jurídico tradicional.

- Por último, los marcos regulatorios sobre el uso de *spyware* deben establecer disposiciones específicas para la protección de comunicaciones entre abogados y clientes, de las fuentes periodísticas y de otras relaciones amparadas por el deber de confidencialidad, como los profesionales médicos respecto de sus pacientes. Dada la capacidad de estas herramientas para capturar información de manera indiscriminada, la protección de estos ámbitos no puede quedar librada a la buena fe de quienes ejecutan la medida, sino que requiere de salvaguardas técnicos y procedimentales.

En conjunto, estas recomendaciones apuntan a un objetivo que trasciende la regulación del *spyware* en sentido estricto: la construcción de un modelo de gobernanza de tecnologías de vigilancia que sea compatible con las exigencias del Estado de derecho. Ese modelo no puede fundarse en la confianza en el buen uso de las herramientas disponibles, sino en el diseño institucional de controles que operen con independencia de la voluntad de quienes las utilizan.

La legitimidad del uso estatal del *spyware* no se presume, sino que debe construirse de manera integral y a lo largo de todo el ciclo de vida de la herramienta.



Cuándo Preocuparse

CUÁNDO PREOCUPARSE

Breve guía para personas que sospechan que pueden estar vigiladas con el uso de *spyware*.

Este apartado presenta cuáles son los indicios críticos a tener en cuenta porque podrían estar asociados a la presencia de *spyware* en nuestros dispositivos.

El hecho de que no se conozcan casos no significa que estas herramientas no estén en uso, por eso está bien tomar precauciones para protegernos y para denunciar si aparece alguno.

El *spyware* o software espía es un tipo de software malicioso que interfiere en el funcionamiento normal de un dispositivo para recopilar información sin alertar a la persona usuaria y después la envía a otra entidad no autorizada. Un dispositivo puede ser infectado de tres maneras:

1. Introduciendo el virus directamente en el dispositivo (para lo cual una persona extraña tiene que tener acceso físico al mismo).

2. Abriendo o descargando un enlace o archivo malicioso ("ataque de 1 click").

3. De manera remota, a través de Internet, aprovechando vulnerabilidades en aplicaciones de mensajería populares como *iMessage* o *WhatsApp* ("ataque de 0 click").

Prevención de ataques

Existen mecanismos y rutinas de seguridad que disminuyen la vulnerabilidad ante ataques de este tipo y los vuelven mucho más difíciles y costosos. Entre ellos se encuentran:

- Mantener actualizados los navegadores y sistemas operativos de los dispositivos, así como las aplicaciones y programas que en ellos se ejecutan.

- Instalar aplicaciones y programas provenientes de tiendas oficiales y fuentes confiables.

- Utilizar contraseñas únicas y con renovaciones periódicas.
- Configurar en los dispositivos doble factor de verificación o multi factor de verificación.
- Configurar el PIN de seguridad de la línea telefónica.
- Revisar con cierta frecuencia los dispositivos conectados de sus mensajerias.
- Tener sumo cuidado de no clickear en enlaces de procedencia desconocida. En caso de dudas, confirmar su fuente a través de otro canal de comunicación de confianza u oficial.
- Prestar atención a cambios en el funcionamiento del dispositivo (ver más abajo ejemplos de esto).
- Reiniciar el dispositivo una vez al día puede mitigar ataques avanzados.
- Minimizar la información sensible almacenada en los dispositivos en la medida de lo posible.

Indicios de posibles ataques

En caso de registrar algunas de las siguientes situaciones, se recomienda realizar un análisis de los dispositivos para evaluar posibles infecciones:

- Si aparecen notificaciones de ataques y/o alertas de seguridad del dispositivo o de cuentas de servicio de confianza (*Facebook, Google, Whatsapp, Apple*, etc).
- Si hubo algún acceso físico no consentido a los dispositivos (por ejemplo, en casos de detenciones o allanamientos).
- Si se confirma que alguien de tu organización, partido, empresa fue infectado con *spyware.*
- Si se producen filtraciones de conversaciones privadas.

- Si aparecen dispositivos desconocidos vinculados en tus mensajerías y redes.
- Si aparecen apps extrañas o no reconocidas.
- Si se produjo un clickeo en un link potencialmente malicioso.
- Si se produce un gasto de batería inesperado.
- Si el equipo se recalienta cuando no está en uso

Autodiagnósticos y pasos a seguir:

- https://digitalfirstaid.org/es/topics/surveilled/
- https://securityplanner.consumerreports.org/es/

Organizaciones que brindan apoyo:

- https://securitylab.amnesty.org/
- https://www.accessnow.org/help/
- https://digitalrightsfoundation.pk/
- https://citizenlab.ca/
- https://dslua.org/
- https://www.eff.org/
- https://www.frontlinedefenders.org/emergency-contact
- https://vita-activa.org/

Vía Libre · DEMOCRACIA EN RED · O.D.I.A. · CELS · newventurefund