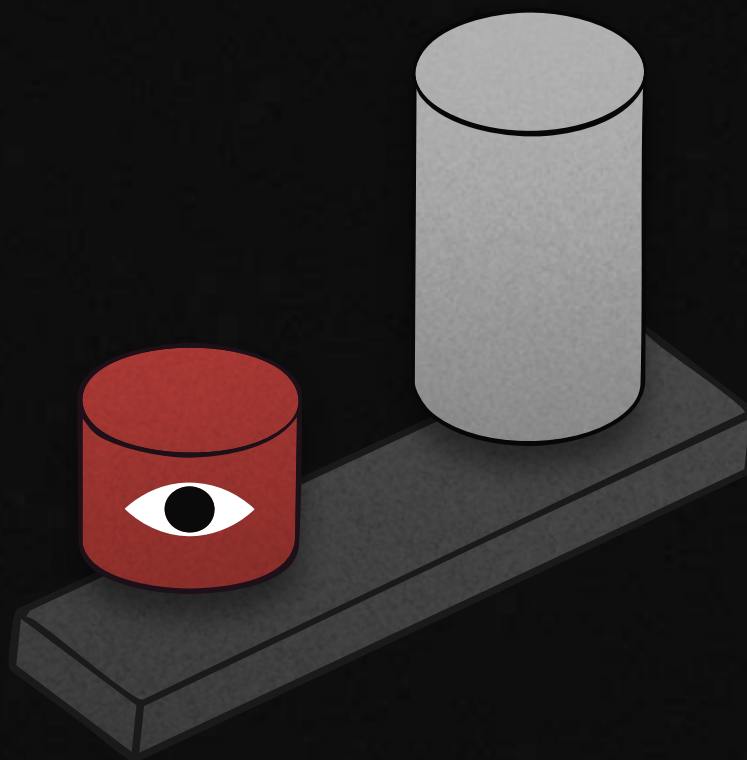


0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

/SPYWARE:

RECOMENDACIONES PARA REGULACIÓN, CONTROL, Y COMPRAS ESTATALES

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



Centro de Estudios Legales y Sociales (CELS),
Democracia en Red, Fundación Vía Libre y
Observatorio Argentino de Derecho Informático (O.D.I.A.).

Realizado con el apoyo de Spyware Accountability Initiative.

Buenos Aires, junio de 2026.

ÍNDICE

4	Resumen ejecutivo
6	Introducción
9	El spyware como tecnología
12	La tensión estructural
15	Riesgos estructurales del spyware
19	El problema institucional
23	El agravante estructural
26	Nivel I: adquisición de sistemas de spyware
31	Nivel II: habilitación judicial del uso de spyware
35	Nivel III: uso operativo y administrativo del spyware
39	Articulación entre niveles

ÍNDICE

44	Lineamientos de política pública
46	Recomendaciones específicas
46	Adquisición
48	Habilitación Judicial
49	Ejecución
52	Retención y destrucción
53	Supervisión
55	Conclusiones

RESUMEN EJECUTIVO

La expansión de la vida social en entornos digitales y la generalización del cifrado han transformado de manera significativa las capacidades de investigación penal. En este nuevo contexto, las técnicas tradicionales de interceptación de comunicaciones han visto reducida su eficacia, generando incentivos para el desarrollo y la adopción de herramientas de acceso directo a dispositivos, comúnmente denominadas *spyware*.

Estas tecnologías introducen un nivel de intrusión cualitativamente distinto, al permitir el acceso amplio y persistente a la información contenida en los dispositivos de las personas, incluyendo comunicaciones, datos personales y, potencialmente, información de terceros. Su utilización plantea desafíos específicos en términos de legalidad, proporcionalidad y control que exceden los marcos regulatorios tradicionales.

Si bien el derecho procesal contemporáneo ha comenzado a incorporar estándares para la regulación de técnicas de investigación tecnológica, estos desarrollos suelen centrarse en momentos específicos —particularmente en la autorización judicial— sin abordar de manera integral el conjunto del ciclo de vida de estas herramientas, que incluye su adquisición, habilitación y uso operativo.

En este contexto, el problema no radica únicamente en la existencia de vacíos regulatorios, sino en la falta de articulación entre los distintos planos en los que estas tecnologías son incorporadas y utilizadas por el Estado. La regulación de su adquisición, las condiciones de su habilitación judicial y los protocolos de su uso operativo suelen desarrollarse de manera separada, bajo estándares que no necesariamente se encuentran alineados.

Esta dinámica adquiere particular relevancia en sistemas federales, donde la distribución de competencias en materia de seguridad, regulación procesal y administración implica que aspectos críticos del ciclo de vida del *spyware* —como los regímenes de contratación pública y los códigos procesales que regulan su uso— sean definidos a nivel subnacional. En ausencia de mecanismos adecuados de coordinación y estándares comunes, esta distribución puede dar lugar a la coexistencia de regímenes heterogéneos, ampliando las superficies de riesgo y dificultando la supervisión efectiva.

En América Latina, además, la incorporación de tecnologías altamente intrusivas se produce en contextos institucionales caracterizados por mecanismos de control aún en consolidación y por antecedentes de uso expansivo de facultades de vigilancia¹, lo que incrementa los desafíos asociados a su implementación.

En este marco, el riesgo no radica únicamente en la capacidad intrusiva del spyware, sino en su implementación bajo regímenes fragmentados y desarticulados. El problema central que aborda este documento es, por tanto, la ausencia de un enfoque integrado que permita gobernar estas tecnologías de manera coherente a lo largo de todas sus etapas, estableciendo condiciones claras de legalidad, control y responsabilidad institucional.

El problema del spyware no es solo tecnológico ni exclusivamente jurídico, sino de gobernanza. Su implementación bajo regímenes fragmentados -especialmente en sistemas federales- amplifica los riesgos de uso indebido. Su regulación exige, por tanto, un enfoque integrado que alinee estándares en la adquisición, la habilitación procesal y el uso operativo, además de establecer salvaguardas particulares en relación a la protección de fuentes y a las comunicaciones entre abogados y clientes.

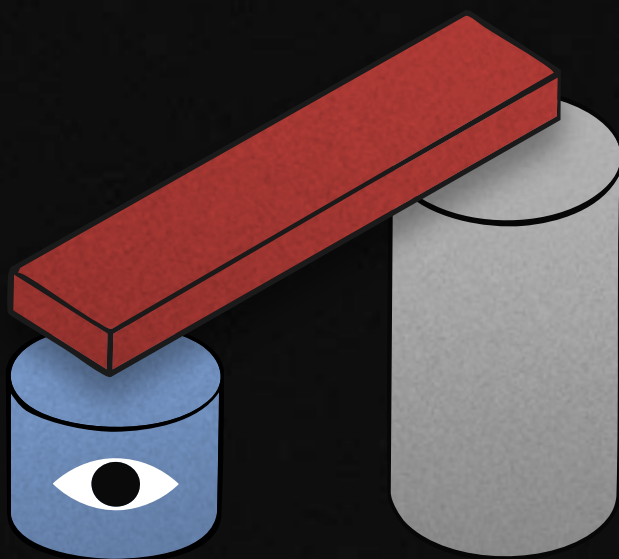
1 Ver. <https://repositorio.mpd.gov.ar/jspui/handle/123456789/4658>

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

INTRODUCCIÓN:

TRANSFORMACIÓN TECNOLÓGICA Y RECONFIGURACIÓN DE LAS CAPACIDADES DE INVESTIGACIÓN

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



INTRODUCCIÓN: TRANSFORMACIÓN TECNOLÓGICA Y RECONFIGURACIÓN DE LAS CAPACIDADES DE INVESTIGACIÓN

La expansión de la vida social en entornos digitales ha modificado de manera profunda las condiciones en las que se desarrollan las actividades de investigación penal. Este cambio no es solo tecnológico: redefine el alcance y los límites de la intervención estatal. Una parte sustantiva de las comunicaciones, las interacciones y la evidencia relevante para la persecución de delitos se produce hoy a través de dispositivos y plataformas digitales, desplazando progresivamente los espacios tradicionales de observación e intervención. Esta transformación resulta particularmente significativa en el contexto de investigaciones de delitos complejos, donde la obtención de evidencia digital se vuelve central.

Al mismo tiempo, la generalización del uso de mecanismos de cifrado —en particular, el cifrado de extremo a extremo— ha transformado la arquitectura de las comunicaciones, limitando el acceso a su contenido durante la transmisión. Este cambio ha reducido la eficacia de técnicas clásicas de investigación, generando un desfase creciente entre las herramientas disponibles y las condiciones tecnológicas en las que se desarrollan muchas actividades delictivas. En este contexto, se configura una dinámica de adaptación recíproca, cercana a una “carrera tecnológica”, en la que el fortalecimiento del cifrado impulsa el desarrollo de técnicas cada vez más intrusivas de acceso a la información.

Frente a estos límites, se observa un desplazamiento progresivo desde la interceptación de comunicaciones hacia el acceso directo a los dispositivos. Este cambio de foco —de la comunicación al dispositivo— no sólo redefine las técnicas de investigación, sino también el alcance de la intervención estatal sobre la vida privada, habilitando el uso de herramientas altamente intrusivas, como el spyware, capaces de obtener información antes o después de que esta sea protegida por mecanismos de cifrado.

Este desplazamiento no es meramente técnico. Supone una reconfiguración de las capacidades estatales de investigación que amplía de manera significativa el alcance potencial de la intervención sobre la vida privada, al tiempo que introduce nuevos desafíos en términos de integridad, trazabilidad y validez de la evidencia obtenida por medios digitales. Esta transformación

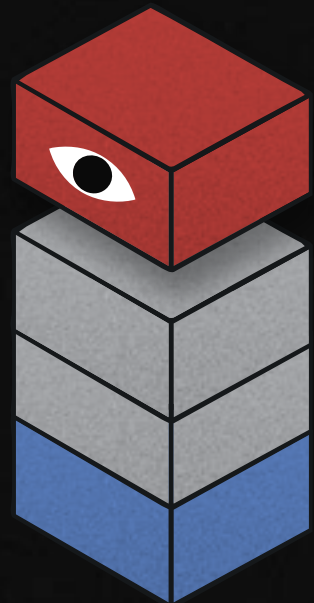
se produce, además, en un contexto en el que los desarrollos tecnológicos avanzan a un ritmo más acelerado que los procesos de rediseño institucional, generando un desfase estructural entre las nuevas capacidades de acceso a la información y los mecanismos disponibles para su regulación y control.

En este escenario, el desafío no radica únicamente en la existencia de estas herramientas, sino en las condiciones bajo las cuales pueden ser utilizadas. La incorporación de capacidades altamente intrusivas en contextos de desalineación normativa y limitaciones institucionales incrementa los riesgos de uso indebido y dificulta la supervisión efectiva. Estos factores no solo afectan la protección de derechos individuales, sino que también inciden sobre la capacidad del sistema institucional para sostener mecanismos adecuados de control, supervisión y rendición de cuentas frente al ejercicio del poder estatal.

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

EL SPYWARE COMO TECNOLOGÍA: DEFINICIÓN, FUNCIONAMIENTO Y ESPECIFICIDAD

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



EL SPYWARE COMO TECNOLOGÍA: DEFINICIÓN, FUNCIONAMIENTO Y ESPECIFICIDAD

El “spyware” designa un tipo de herramienta tecnológica que permite acceder de manera subrepticia al contenido y funcionamiento de dispositivos digitales, habilitando un rango de intervención significativamente más amplio que el de las técnicas tradicionales de investigación. En el contexto de la investigación penal, estas herramientas se caracterizan por permitir la captación de datos mediante la intervención directa sobre el dispositivo de la persona investigada. No se trata de una técnica más dentro del repertorio investigativo, sino de una capacidad de acceso integral al entorno digital de una persona.

El desarrollo de estas herramientas no es reciente. Sus antecedentes pueden rastrearse en tecnologías de vigilancia utilizadas por agencias de inteligencia desde principios de la década de 2000, inicialmente orientadas a operaciones específicas y de alto valor. Sin embargo, en los últimos diez años se ha producido una expansión significativa de su uso y disponibilidad, impulsada por la consolidación de un mercado global de software de intrusión comercializado por empresas especializadas y adquirido por agencias estatales. Esta evolución ha transformado al spyware en una tecnología cada vez más accesible, con capacidades estandarizadas y circulación transnacional, lo que amplía su impacto potencial y complejiza los desafíos asociados a su regulación.

A diferencia de otras técnicas de investigación, el uso de spyware no se limita a la observación o captación de información disponible en redes o sistemas externos, sino que implica la ejecución de acciones técnicas sobre el propio dispositivo, destinadas a habilitar el acceso al sistema y a la información que este contiene. En este sentido, su funcionamiento se aproxima al de ciertas formas de intrusión informática, en la medida en que requiere intervenir el dispositivo para permitir el acceso remoto a sus datos. Lejos de limitarse a captar información, posibilita intervenir el entorno digital completo de una persona.

Desde un punto de vista funcional, el spyware puede ser entendido como una forma avanzada de software de acceso remoto (Remote Access Tools o RAT), que permite la toma de control encubierta de dispositivos y el acceso

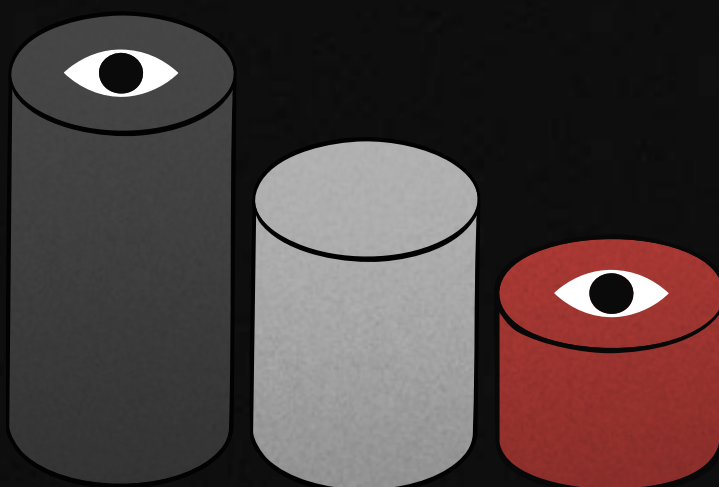
a comunicaciones, archivos, registros de actividad y datos almacenados, así como también pueden permitir la activación de funciones del dispositivo, lo que amplía significativamente el alcance potencial de la información que puede obtenerse. A su vez, una característica distintiva de estas herramientas es su capacidad de operar de manera persistente en el tiempo, manteniendo el acceso al dispositivo sin conocimiento de la persona afectada.

La eventual habilitación legal de estas herramientas no altera su naturaleza técnica. Aun cuando su utilización pueda encontrarse autorizada en determinados contextos, el spyware supone la realización de acciones intrusivas sobre el dispositivo de una persona, ya que la explotación de vulnerabilidades del dispositivo es una condición necesaria para obtener acceso al sistema y a la información que este contiene. En conclusión, el uso de spyware presenta un alto grado de opacidad, tanto en su funcionamiento técnico como en sus efectos. La complejidad de estas herramientas, sumada a su carácter encubierto, dificulta la verificación independiente de su utilización, la trazabilidad de las acciones realizadas y la delimitación precisa de la información efectivamente recolectada. En conjunto, estas características constitutivas del spyware configuran una capacidad de acceso integral, persistente y difícilmente auditable, que plantea desafíos regulatorios cualitativamente distintos a los de otras técnicas de investigación.

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

LA TENSIÓN ESTRUCTURAL: CIFRADO, PODER ESTATAL Y DESPLAZAMIENTO HACIA LA INTRUSIÓN

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



LA TENSIÓN ESTRUCTURAL: CIFRADO, PODER ESTATAL Y DESPLAZAMIENTO HACIA LA INTRUSIÓN

El cifrado de extremo a extremo no constituye una transformación meramente técnica, sino también estructural, en tanto altera la arquitectura de poder sobre la información. En el modelo tradicional de comunicaciones, el intermediario tenía acceso al contenido en texto plano. Eso significa que podía ser compelido —en principio por orden judicial— a colaborar y entregarlo en el marco de una investigación. La irrupción del cifrado de las comunicaciones eliminó la posibilidad de que un intermediario pueda conocer su contenido, en tanto éste verá sólo datos encriptados que no pueden descifrarse sin la clave correspondiente, por lo que este cambio ha terminado por modificar la arquitectura sobre la que operan el derecho, el mercado y el poder estatal. En el esquema actual la comunicación existe, en sentido técnico, solo en los dispositivos de los extremos, por lo que la consecuencia inmediata es un desplazamiento irreversible del paradigma de acceso estatal conocido hasta el momento.

En el marco de una investigación existe como recurso la interceptación de las comunicaciones en tránsito, conocida en la jerga informática como “ataque MITM” o “Man In The Middle”. En la actualidad, al no poder interceptarse las comunicaciones debido a que el texto en tránsito se encuentra cifrado, este mecanismo carece de eficacia, volviéndose operativamente inútil. La respuesta institucional fue la reorientación hacia la infiltración: hoy en día no se busca acceder al canal en sí, sino a alguno de los dispositivos que se encuentran en los extremos de la comunicación. Técnicas como el *lawful hacking* o la instalación de software espía en el terminal del objetivo no son evoluciones de la interceptación clásica, sino que constituyen una sustitución de la misma por una forma radicalmente distinta de vigilancia.

Aquí emerge una distinción que el ordenamiento jurídico no suele abordar con la nitidez necesaria: acceso al dispositivo y acceso a la comunicación son intervenciones jurídicamente heterogéneas. La segunda afecta el mensaje en su transmisión; la primera implica el control funcional sobre una esfera privada mucho más amplia, ya que como se expuso anteriormente accede a la ubicación, historial, contactos, documentos, fotografías o conversaciones no relacionadas con el objeto de investigación, llegando incluso a afectar a terceros ajenos al proceso o a activar de manera remota funciones del

propio dispositivo. Tratarlas como equivalentes o análogas desde el punto de vista de los requisitos de autorización produce una asimetría gravísima entre el umbral procesal exigido y la magnitud real de la intrusión.

En este sentido, su implementación conlleva serias implicancias institucionales. Los marcos de habilitación previstos para la interceptación clásica fueron diseñados para una operación acotada y pasiva, mientras que la infiltración de dispositivos es activa, potencialmente persistente y de alcance ilimitado. Sin embargo, la presión por mantener capacidades de investigación y vigilancia efectivas frente a la adopción generalizada del cifrado incentiva este cambio de paradigma que parece no tener vuelta atrás. Es importante aclarar que el cifrado no creó el problema, sino que lo evidenció. La tensión entre acceso legítimo del Estado y la privacidad de las comunicaciones siempre existió, incluso desde los tiempos de la correspondencia epistolar. El cifrado de extremo a extremo simplemente hizo que el sistema anterior dejara de funcionar por defecto, volviendo a sacar a la luz el debate sobre la pugna entre las capacidades estatales de investigación y vigilancia y la privacidad de los ciudadanos.

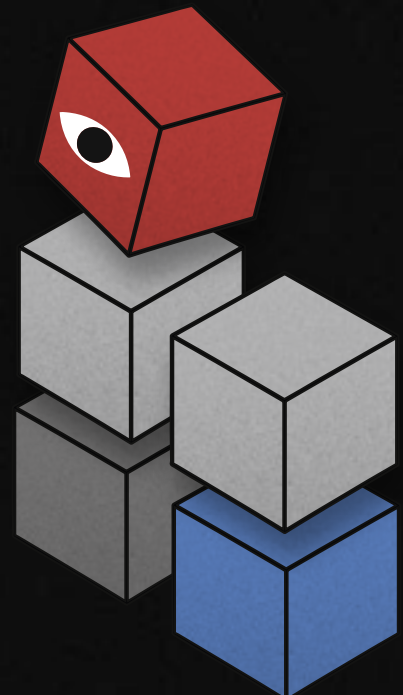
Como bien anticipaba Hairabedián, *“La intervención telefónica por su vía tradicional muchas veces es ineficaz para conocer las comunicaciones del investigado. Ya sea porque cambia de línea constantemente (chip o sim), o utiliza sistemas de comunicación de difícil acceso o servicios de chat o mensajería cifrados o con mecanismos para protegerlo de la intromisión externa(...) a veces la única alternativa es la colocación directa o remota de un programa oculto en el aparato móvil para la extracción y transmisión de todas las comunicaciones o inclusive el acceso a fotografías, videos y documentos. Lo problemático es si en nuestro sistema un juez, al ordenar la intervención de las comunicaciones del imputado, por el fracaso en el método, puede autorizar que se la materialice con la colocación de spywares (p. ej., un “troyano” que remita la información a una cuenta de correo electrónico o dirección IP)²”*.

2 Maximiliano Hairabedián - El acceso a información y datos de teléfonos celulares, Página 20, Punto 8 “Acceso mediante spywares”

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

RIESGOS ESTRUCTURALES DEL SPYWARE

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



RIESGOS ESTRUCTURALES DEL SPYWARE

Este spyware, también llamado *Troyano Estatal*, presenta una constelación de riesgos estructurales que lo distinguen cualitativamente de cualquier otra técnica de investigación intrusiva conocida por el derecho procesal clásico. Esos riesgos no necesariamente son subsanables mediante una regulación más cuidadosa, sino que son inherentes a la naturaleza técnica de la herramienta y a la arquitectura sobre la que opera. Sin perjuicio de ello, es fundamental que exista una coordinación entre las distintas etapas de su ciclo para poder morigerar sus potenciales efectos dañosos. Un análisis serio sobre las características inherentes al spyware exige considerar al menos las dimensiones de riesgo más problemáticas, a saber:

En primer término, la interceptación tradicional de comunicaciones opera sobre un objeto acotado: el contenido de una comunicación en tránsito. Su objeto es concreto, su alcance es definible *ex ante* y su ejecución no altera el dispositivo ni el entorno del investigado o de potenciales terceros que puedan verse afectados por la medida. El spyware, por el contrario, opera sobre el dispositivo en su totalidad. Es decir que una vez es instalado accede potencialmente a la integridad de la vida digital del sujeto, ya sea desde mensajes, correos, documentos o fotografías, pasando por el historial de navegación, contraseñas almacenadas, contactos, calendario y notas de voz; hasta incluso el historial de ubicaciones. Asimismo, existen herramientas de la clase de Pegasus —desarrollado por NSO Group— que pueden ir aún más lejos, ya que posibilitan activar el micrófono y la cámara en tiempo real, convirtiendo el dispositivo en un instrumento de vigilancia ambiental continua. En este sentido, la fina línea entre intervención de comunicaciones y vigilancia continua acaba por desdibujarse, en tanto el teléfono intervenido se vuelve simultáneamente una escucha, un registro domiciliario y un acceso remoto a archivos privados, ejecutados de modo permanente y sin límite conocido. La injerencia no es acotada sino totalizante, y esa diferencia de grado constituye una diferencia trascendental de naturaleza desde el punto de vista de las garantías constitucionales comprometidas.

En segundo lugar, las técnicas de investigación intrusiva clásicas tienen costos marginales crecientes, debido a que cada nueva interceptación requiere tanto de una orden judicial individualizada en el marco de un proceso como de una infraestructura técnica específica para el caso particular.

Estos costos, sumados al procedimiento legal, terminan operando como un límite a la vigilancia masiva. El spyware rompe esa restricción ya que una vez que la herramienta es adquirida, desplegarla posteriormente sobre un dispositivo adicional tiene un costo marginal cercano a cero. En ese sentido, la escala potencial del spyware no constituye un riesgo teórico sino una tendencia empíricamente verificada.

Siguiendo con lo expuesto, esta escala potencial también deriva en una concreta afectación a terceros, ya que el spyware instalado en un dispositivo no interviene únicamente el dispositivo investigado, sino que también interviene las comunicaciones con todos sus interlocutores, ninguno de los cuales necesariamente es objeto de la investigación ni ha sido individualizado en la orden de autorización. No importa si es un amigo, un abogado defensor, un médico, un periodista o un familiar; en principio todos quedan expuestos en el contenido de sus comunicaciones con el investigado sin que ninguna orden judicial los haya alcanzado y sin que tengan conocimiento ni posibilidad de cuestionar la medida. Esta afectación colateral es estructural, por tanto, es inherente a la naturaleza invasiva de la herramienta y no puede ser evitable mediante su diseño, ya que además deriva directamente del hecho de que en la actualidad las comunicaciones sean cifradas de extremo a extremo, de que el dispositivo las almacene en su totalidad e integridad y de que las mismas puedan llegar a ser incluso multilaterales o grupales.

A su vez, otro aspecto importante a tener en cuenta es la opacidad y la dificultad de control de estas herramientas, tanto anterior como posterior. Tradicionalmente, el control judicial de las medidas de investigación suponía que el Juez que autorizaba la medida podía definir su objeto, verificar que su ejecución se ajustó a lo autorizado y, en su caso, declarar la nulidad de lo actuado en exceso. Sin embargo, el spyware hace imposible ese control en cada uno de sus momentos. Al momento de la autorización el juez no puede definir con precisión qué capturará el software, ya que eso dependerá de las capacidades técnicas de cada herramienta, que el juez no controla ni comprende en detalle. Durante la ejecución, el software opera de modo enteramente opaco, en tanto a priori no genera registros auditables por terceros, no notifica al investigado, ni produce logs verificables independientemente. Al momento del control ex post, ni el juez ni la defensa pueden verificar si el software capturó solo lo autorizado o excedió el mandato, porque el acceso al código fuente y a los registros de la operación está en manos del proveedor o de la fuerza de seguridad, que

tienen incentivos para no revelarlos tales como la “propiedad intelectual sobre el modelo” o la “confidencialidad de la operación”, respectivamente. Esta opacidad, lejos de ser un defecto de implementación, se vuelve una característica estructural del modelo; sumado a que los proveedores de spyware comercial consideran a sus herramientas secretos industriales y se niegan sistemáticamente a revelar su funcionamiento interno incluso ante requerimientos judiciales. El control judicial se convierte así en una formalidad sin contenido sustantivo, lo que compromete la legitimidad constitucional de la medida desde su base.

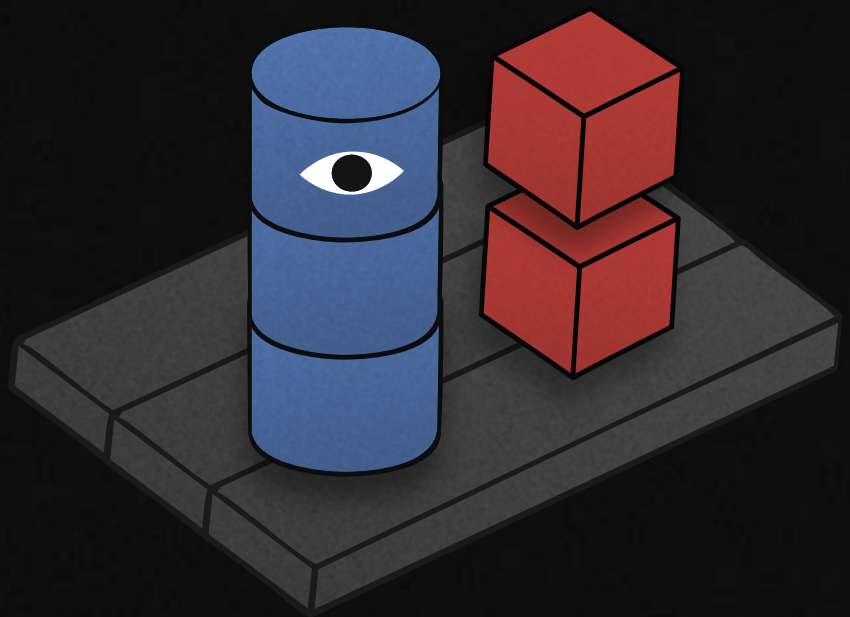
Por último, el spyware también enfrenta problemas probatorios y de integridad de la evidencia. La cadena de custodia digital exige poder demostrar que la evidencia no fue alterada desde su captura hasta su presentación en juicio, pero el spyware opera interviniendo un dispositivo activo, modificando su estado, hasta instalando componentes que interactúan con el sistema operativo y con las aplicaciones. Por tanto, hasta podría decirse que la mera presencia del software en el dispositivo altera el objeto sobre el que opera, contaminando potencialmente la evidencia que recolecta. A ello se suma que la evidencia digital capturada por el software es producida unilateralmente por la parte acusadora, sin posibilidad de que la defensa observe, verifique o contradiga el proceso de recolección. En los sistemas procesales que admiten el principio de igualdad de armas como garantía constitucional esto genera una asimetría probatoria desde la génesis de la medida, sumado a que actualmente tampoco está muy claro cuál es el alcance de la doctrina de la Plain View en ámbitos digitales, o incluso siquiera si puede ser de aplicación dada su incapacidad material de aplicarse análogamente a los dispositivos tecnológicos³. La integridad de la evidencia producida por spyware no puede ser verificada sin acceso al código fuente y a los logs de operación, que en la práctica nunca están disponibles para la defensa, por tanto en principio no puede acreditarse que no se haya manipulado el contenido o incluso incorporado otro de manera externa y espuria.

3 Ver. <https://www.saij.gob.ar/DACF240060>

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

EL PROBLEMA INSTITUCIONAL: LA GOBERNANZA MULTINIVEL DEL SPYWARE

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



EL PROBLEMA INSTITUCIONAL: LA GOBERNANZA MULTINIVEL DEL SPYWARE

El análisis de los riesgos asociados al uso de spyware no puede agotarse en su dimensión técnica ni en los problemas que plantea su habilitación jurídica. Incluso si se asumiera la existencia de marcos normativos adecuados para autorizar su uso en casos concretos, subsiste una dificultad más profunda vinculada a la forma en que estas herramientas son incorporadas, gestionadas y utilizadas por el Estado. El problema del spyware no es solo tecnológico ni exclusivamente jurídico, sino fundamentalmente un problema de organización institucional.

A diferencia de otras técnicas de investigación, el spyware no se integra al aparato estatal a través de una única decisión ni bajo un único régimen jurídico. Su implementación se desarrolla a lo largo de un conjunto de etapas que involucran actores distintos y marcos normativos diferenciados. Este ciclo comprende, al menos, la adquisición de la herramienta, su habilitación en el marco de un proceso judicial y su utilización efectiva por parte de las agencias encargadas de la investigación. Asimismo, este proceso no resulta meramente secuencial, sino que define la forma en que el Estado ejerce, limita o pierde el control sobre estas herramientas. Cada una de estas instancias responde a lógicas propias, se encuentra regulada por normas diferentes y es ejecutada por actores que no necesariamente comparten criterios, capacidades ni incentivos.

Esta fragmentación interna no constituye un problema meramente organizativo, sino que tiene efectos directos sobre la posibilidad de ejercer un control efectivo sobre la implementación y uso de estas herramientas. La adquisición de sistemas ofensivos suele regirse por normas de contratación pública que no están diseñadas para evaluar los riesgos específicos asociados a tecnologías de intrusión. La habilitación judicial, por su parte, se enfoca en la justificación de la medida en un caso concreto, sin necesariamente tener en cuenta las características técnicas de la herramienta utilizada ni sus implicancias operativas. Finalmente, la ejecución de la medida queda en manos de las fuerzas de seguridad o de investigación, que operan bajo protocolos propios y con márgenes de discrecionalidad difíciles de supervisar desde el plano judicial.

Esta distribución funcional resulta en que ninguna de las instancias involucradas controla de manera integral el ciclo de vida de la herramienta. Lo que se compra no siempre se corresponde con lo que se autoriza, y lo que se autoriza no necesariamente coincide con lo que efectivamente se ejecuta. Esta desalineación no agota sus efectos al marco organizativo sino que debilita de manera sustancial la capacidad del Estado para ejercer un control sobre la utilización de herramientas de alta intrusión. Se generan así zonas de opacidad que dificultan la trazabilidad de las decisiones y se erosionan los mecanismos tradicionales de rendición de cuentas al mismo tiempo que, irónicamente, se habilita la adquisición de estos sistemas.

En este contexto, el problema no radica únicamente en la existencia de vacíos regulatorios, sino en la ausencia de un enfoque integrado que permita articular estos distintos planos de decisión bajo criterios comunes. La regulación aislada de cada etapa resulta insuficiente frente a una tecnología que, por su propia naturaleza, atraviesa y conecta múltiples dimensiones de la acción estatal. Sin la definición de estándares integrados que abarquen la totalidad del ciclo de vida de la herramienta, los distintos niveles de regulación tienden a operar de manera inconexa, haciendo inviable un control efectivo.

A ello se suma un elemento adicional que complejiza aún más el escenario. En la práctica, el control efectivo sobre el funcionamiento de estas herramientas tiende a desplazarse hacia los actores que detentan el conocimiento técnico y la capacidad operativa para implementarlas. Esto incluye tanto a las agencias estatales especializadas como, en muchos casos, a los propios proveedores de la tecnología en cuestión. En este escenario, son estos actores quienes terminan definiendo, en los hechos, el alcance efectivo de la intervención, incluso más allá de los términos formales de su autorización. Esto se ve reforzado por la creciente intermediación técnica que caracteriza a estas herramientas, la cual dificulta que las instancias tradicionales de control puedan comprender, verificar y acompañar su funcionamiento en tiempo real. Como resultado, la función de control y gobernanza en cabeza de los poderes públicos se ve progresivamente erosionada, en la medida en que los operadores jurídicos carecen, en muchos casos, de las capacidades técnicas necesarias para ejercer una supervisión sustantiva sobre sistemas cuya complejidad excede los marcos tradicionales de formación institucional.

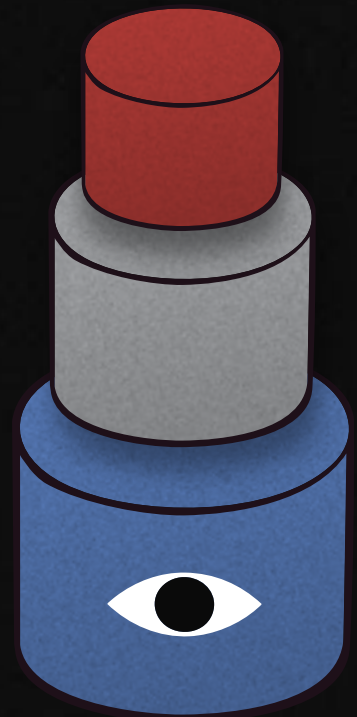
En ausencia de una articulación efectiva entre los distintos niveles involucrados, el uso de spyware queda, en los hechos, condicionado por la

capacidad técnica y operativa de quienes lo implementan, antes que por los límites formales establecidos por el derecho. En consecuencia, el desafío que plantea esta tecnología no puede ser abordado únicamente mediante ajustes puntuales en el derecho procesal o en los regímenes de contratación. Requiere, en cambio, un enfoque de gobernanza que reconozca la interdependencia entre las distintas etapas de su implementación y que permita establecer estándares coherentes a lo largo de todo su ciclo de vida. Sin esta articulación, incluso los marcos normativos más exigentes corren el riesgo de resultar insuficientes frente a una tecnología cuyo impacto excede los límites de cualquier regulación sectorial. Esta problemática se vuelve aún más compleja en contextos institucionales en los que las funciones involucradas se encuentran distribuidas entre distintos niveles de gobierno, como ocurre en los sistemas federales.

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

EL AGRAVANTE ESTRUCTURAL: IMPLEMENTACIÓN EN SISTEMAS FEDERALES

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



EL AGRAVANTE ESTRUCTURAL: IMPLEMENTACIÓN EN SISTEMAS FEDERALES

La arquitectura institucional del federalismo introduce una capa adicional de complejidad cuando se contratan y ejecutan este tipo de herramientas. Atento a que en nuestro país cada provincia establece a través de su propio código de forma el régimen de adquisición y autorización para la interceptación de comunicaciones, es dable observar que terminen coexistiendo no solamente umbrales de protección distintos, sino también definiciones divergentes, marcos de responsabilidad incompatibles y hasta empresas proveedoras diferenciadas.

A su vez, esto es agravado por la multiplicidad de actores, debido a que en el plano estatal conviven fuerzas de seguridad nacionales, provinciales y locales, organismos de inteligencia con mandatos diferenciados, fiscalías con distintos grados de independencia, y jueces con competencias materiales y territoriales que no siempre coinciden con la naturaleza de las comunicaciones digitales, que son por definición interjurisdiccionales. En este sentido, cada uno de estos actores opera con sus propias jerarquías de mando, sus propios protocolos de solicitud y sus propias relaciones con los proveedores de servicios.

Esta multiplicidad de actores también da cuenta de una potencial asimetría de capacidad técnica entre jurisdicciones, que quizá es un factor menos visible pero no por ello menos determinante. Las agencias de inteligencia o las provincias con más recursos suelen concentrar las capacidades técnicas sofisticadas —ya sea por el acceso a las herramientas o por su conocimiento actualizado de vulnerabilidades en los dispositivos—, mientras que otras fuerzas provinciales o locales carecen de ellas. Esto crea dependencias verticales informales que terminan operando al margen de los marcos normativos de cooperación y generando incentivos para que existan ciertos actores que busquen delegar operaciones que excedan su competencia formal. Paradójicamente, esta fragmentación normativa y la asimetría de capacidad técnica que conlleva, también son permeables a los desvíos regulatorios, por ejemplo cuando los requisitos de autorización son más exigentes en una jurisdicción que en otra. En ese caso, una investigación que utilice un spyware que no superaría el estándar de proporcionalidad federal podría intentarse mediante una fiscalía provincial con un umbral más bajo.

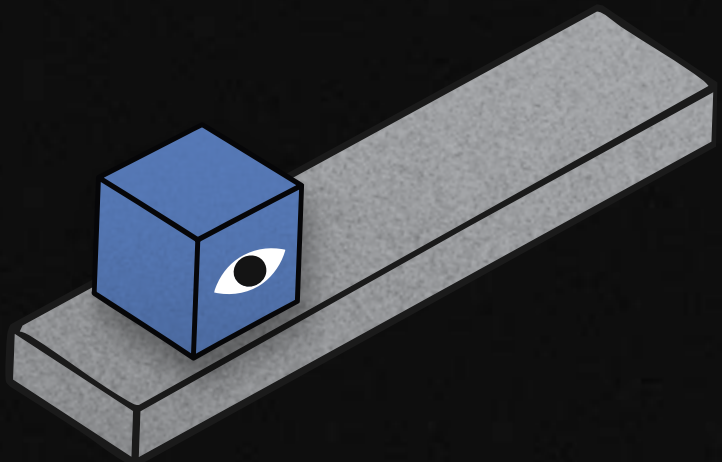
Por último, el hecho de que cada actor pueda adquirir una licencia de software específica y distinta de los otros implica que es prácticamente imposible poder garantizar parámetros mínimos de seguridad y trazabilidad que sean aplicables en todo el territorio nacional, debido a que cada empresa proveedora operará con su propio conjunto de reglas y límites. Esto hace que, en línea con lo expuesto, sea menester abordar al spyware de manera integral y a través del análisis de sus tres dimensiones o niveles principales.

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

NIVEL I:

ADQUISICIÓN DE SISTEMAS DE SPYWARE

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



NÚCLEO NORMATIVO

→ NIVEL I: ADQUISICIÓN DE SISTEMAS DE SPYWARE

La discusión pública sobre el uso estatal de spyware suele concentrarse en las condiciones bajo las cuales estas herramientas son autorizadas judicialmente o cómo pueden ser utilizadas como un medio probatorio válido en investigaciones concretas. Sin embargo, buena parte de los problemas asociados a este tipo de tecnologías aparece mucho antes de su despliegue efectivo. En este sentido, el problema no comienza cuando el spyware es utilizado, sino desde el momento en que el Estado decide incorporar este tipo de capacidades a su aparato institucional.

La compra de spyware no funciona como una contratación pública más. Lo que el Estado incorpora en estos casos no es simplemente software, sino capacidades técnicas de vigilancia e intrusión con aptitud para alterar de manera significativa la relación entre el poder estatal y los derechos fundamentales de las personas sometidas a investigación. Así, la contratación pública deja de funcionar únicamente como un mecanismo de adquisición de tecnología y pasa a convertirse también en una instancia de diseño de las capacidades, límites y condiciones técnicas bajo las cuales el Estado ejercerá posteriormente potestades de vigilancia.

Esto adquiere especial relevancia en el marco del régimen nacional de contrataciones públicas. El Decreto 1023/01⁴ y el andamiaje normativo que regula las compras estatales fueron concebidos, en gran medida, para la adquisición de bienes tangibles, prestaciones relativamente estables y objetos susceptibles de verificación material directa. Esa lógica empieza a mostrar límites evidentes cuando se aplica a tecnologías dinámicas y opacas, cuyas capacidades pueden modificarse incluso después de su adquisición mediante actualizaciones —tanto de software como de *firmware*— o cambios de configuración.

En sistemas federales como el nuestro este problema se multiplica, en atención a que la habilitación procesal para utilizar estas herramientas suele depender de regulaciones provinciales, por lo que esa fragmentación termina proyectándose también sobre los regímenes administrativos y de contratación utilizados para adquirirlas. Como resultado, las condiciones bajo las cuales estas capacidades son incorporadas al aparato estatal pueden variar significativamente entre jurisdicciones, generando estándares desiguales en materia de control, auditabilidad y limitación técnica de las herramientas utilizadas.

Es aquí donde se evidencia el problema de fondo: en el modelo clásico de contratación pública primero el Estado incorpora una capacidad y luego regula, controla o sanciona eventuales desviaciones en su utilización. Pero el software, y especialmente herramientas de esta naturaleza, funcionan de otro modo. Buena parte de sus límites, restricciones y mecanismos de control pueden incorporarse desde el propio diseño técnico del sistema. Dicho de otro modo, el problema ya no pasa únicamente por controlar cómo se usa la herramienta, sino por discutir qué tipo de capacidades decide incorporar el Estado, con qué oferentes contratará estas herramientas y bajo qué límites técnicos lo hará.

Esto modifica de manera sustancial la relación entre contratación pública y garantías procesales. En esta línea, es importante señalar que la discusión ya no debería limitarse a si una herramienta puede ser utilizada de manera compatible con los derechos de las personas investigadas, sino también a si su propia arquitectura técnica fue concebida para operar dentro de esos límites desde el comienzo. En tecnologías de esta naturaleza, las garantías no deberían actuar únicamente como restricciones externas al ejercicio del poder estatal, sino como condiciones incorporadas desde el diseño mismo de las capacidades técnicas que el Estado decide adquirir.

A diferencia de lo que ocurre con gran parte de los bienes materiales tradicionalmente incorporados por la administración pública, las tecnologías de spyware permiten integrar mecanismos de limitación funcional, trazabilidad, auditabilidad y control desde el momento mismo de su adquisición e implementación. Aspectos como la existencia de registros verificables de uso, la posibilidad de reconstrucción posterior de operaciones realizadas, la delimitación técnica de alcances funcionales o la incorporación de restricciones automáticas compatibles con estándares de

proporcionalidad y demás salvaguardas específicas pueden formar parte del propio diseño de la herramienta o al menos de las condiciones bajo las cuales el Estado decide contratarla.

Sin embargo, los regímenes tradicionales de contratación pública suelen tratar estas tecnologías como si se tratara de simples bienes informáticos o servicios técnicos convencionales. Bajo esta lógica, las evaluaciones tienden a concentrarse en variables de índole económica o material, dejando en un segundo plano cuestiones vinculadas con la auditabilidad del sistema, la posibilidad de control independiente, la dependencia técnica respecto del proveedor o la compatibilidad de la herramienta con estándares mínimos de control judicial y protección de derechos fundamentales de los nacionales.

Cuando el Estado adquiere herramientas cuya lógica técnica no puede ser plenamente comprendida, auditada o limitada por las propias instituciones que las incorporan, el control efectivo sobre su funcionamiento tiende a desplazarse hacia quienes detentan el conocimiento técnico especializado o el dominio operativo de la herramienta. En estos escenarios, la contratación pública deja de funcionar únicamente como un mecanismo de adquisición de bienes o servicios y pasa a convertirse, en los hechos, en una instancia de incorporación de capacidades estatales de vigilancia parcialmente externalizadas hacia actores privados cuya intervención resulta difícilmente controlable bajo los marcos tradicionales del derecho administrativo.

La situación se vuelve aún más compleja si se considera que muchas de estas herramientas dependen de vulnerabilidades de seguridad o capacidades de explotación técnica cuya existencia y preservación forman parte de su lógica de funcionamiento. Así las cosas, el Estado no termina adquiriendo únicamente software, sino también capacidades sustentadas sobre dinámicas técnicas tercerizadas y difíciles de compatibilizar con esquemas tradicionales de transparencia, auditabilidad y control institucional.

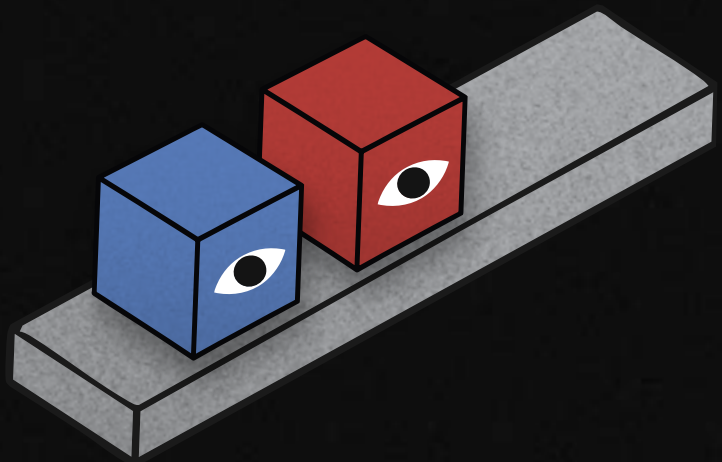
En definitiva, el problema asociado a la adquisición estatal de spyware no radica únicamente en la incorporación de herramientas potencialmente intrusivas, sino también en las condiciones institucionales y técnicas de base bajo las cuales el Estado decide integrarlas a sus estructuras de investigación criminal. Mientras los regímenes de contratación continúen sin abordar los riesgos específicos de estas tecnologías, se perpetúa la imposibilidad de establecer adecuadamente un andamiaje institucional que

permita su correcto despliegue sin potenciales riesgos. De igual manera, este nivel de riesgo no debe escindirse de los siguientes, en tanto los tres conforman de manera integral los aspectos más problemáticos del spyware.

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

NIVEL II: HABILITACIÓN JUDICIAL DEL USO DE SPYWARE

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



NÚCLEO NORMATIVO

→ NIVEL II: HABILITACIÓN JUDICIAL DEL USO DE SPYWARE

Como bien se ha anticipado, la habilitación judicial se enfoca en la justificación de la medida en un caso concreto sin considerar las características técnicas específicas de la herramienta ni sus implicancias de uso. En el análisis de este segundo nivel se postularán elementos que creemos deben ponderarse para poder establecer un régimen procesal que garantice un piso mínimo de derechos, máxime habida cuenta del grado de intrusión de estas herramientas y el nivel de injerencia en derechos fundamentales que acarrearán de forma intrínseca a su funcionamiento.

Ese piso mínimo debe construirse sobre cinco principios rectores, siendo estos los principios de especialidad, idoneidad, necesidad, excepcionalidad y proporcionalidad. La especialidad exige que la medida esté directamente vinculada a la investigación de un delito concreto y determinado, excluyendo toda autorización orientada a descubrir o prevenir delitos sin base objetiva previa. La idoneidad opera como criterio para delimitar el ámbito subjetivo, el ámbito objetivo y la duración de la medida, a partir de una evaluación fundada sobre su utilidad efectiva para la investigación. La necesidad y la excepcionalidad imponen que el uso de la herramienta sea de última ratio, es decir que sólo procederá cuando no existan medidas igualmente útiles para la averiguación de la verdad que resulten menos gravosas para los derechos del imputado, o cuando la persecución del delito se vea gravemente dificultada sin su empleo. La proporcionalidad, finalmente, exige que el sacrificio de los derechos e intereses afectados sea ponderado frente al beneficio que la medida reporta al interés público, tomando en consideración la gravedad del hecho, su trascendencia social o el ámbito tecnológico en que se produjo, la intensidad de los indicios existentes y la relevancia del resultado perseguido.

En atención al grado de restricción de derechos que estas herramientas producen, los delitos que habilitan su uso deben estar enumerados taxativamente en el ordenamiento de fondo, sin dejar su determinación al libre arbitrio del órgano requirente. El estándar comparado ha reconocido como delitos perseguibles mediante herramientas de acceso remoto a los cometidos en el seno de organizaciones criminales; los referidos a actos de terrorismo; los cometidos contra menores o personas con capacidad

restringida; los que afectan la Constitución, la defensa nacional o implican traición; y los cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación.

La habilitación judicial, en tanto resolución que autoriza la medida, debe pronunciarse sin excepción sobre los siguientes extremos: el hecho punible objeto de la investigación y su tipificación, con expresión de los indicios racionales en que se funda; la identidad de los investigados y de cualquier otro afectado por la medida, si fuere conocida; la extensión y el alcance específico de la intervención y la acreditación del cumplimiento de los principios rectores; la duración de la medida; la forma y periodicidad con la que se informará al juez sobre sus resultados; la finalidad perseguida; y la unidad investigadora o el personal a cargo de la ejecución, con indicación del sujeto obligado a colaborar y guardar secreto, bajo apercibimiento de incurrir en desobediencia. Respecto de los registros remotos sobre sistemas informáticos en particular, la resolución debe especificar los dispositivos alcanzados por la medida, el alcance del registro, el software mediante el cual se ejecutará y la forma en que se procederá al acceso y la aprehensión de datos relevantes, indicando si se autoriza la copia y conservación de los datos captados y las medidas necesarias para preservar su integridad. Si en el curso de la ejecución surgen indicios de que los datos buscados se encuentran en un sistema distinto del autorizado, deberá darse inmediata comunicación al juez para que este resuelva sobre una eventual ampliación del objeto de la medida.

La duración de la medida no podrá exceder de un mes, plazo derivado de los estándares comparados en atención a la intensidad de la injerencia. Podrá prorrogarse mediante auto motivado del juez competente por períodos iguales hasta un máximo de tres meses, siempre que subsistan las causas que la motivaron y se haya acompañado un informe detallado del resultado obtenido y de las razones que justifican la continuación. El juez podrá asimismo ordenar el cese anticipado de la medida cuando desaparezcan las circunstancias que justificaron su adopción o resulte evidente que no se están obteniendo los resultados pretendidos.

Una vez finalizado el procedimiento mediante resolución firme, deberá ordenarse el borrado y eliminación de los registros originales obrantes en los sistemas empleados en la ejecución, conservando únicamente una copia bajo custodia judicial que será destruida a los cinco años desde la ejecución

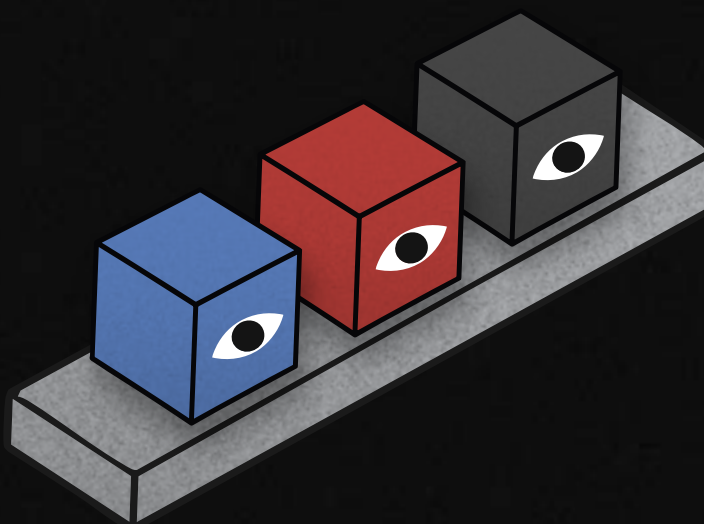
de la pena impuesta, el sobreseimiento, la prescripción o la sentencia firme, según corresponda. Sin perjuicio de ello, el resultado de la medida podrá ser utilizado como medio de prueba en otro proceso penal, siempre que la injerencia haya sido legítima, se haya ajustado al alcance fijado en la resolución que la habilitó y se hayan acreditado los recaudos indispensables en la solicitud respectiva. En tal caso, el juez competente deberá verificar la diligencia de la actuación y evaluar el marco en que se produjo el hallazgo casual.

Estos puntos a tener en cuenta para que una habilitación judicial esté de acuerdo con un piso mínimo que garantice un respeto por los derechos fundamentales demuestran que no pueden aplicarse análogamente los requisitos para las medidas de interceptación tradicionales, toda vez que estos son mucho más acotados y generales derivados de ser pensados y normados para un ámbito analógico o físico. Asimismo, a la adquisición pública del sistema y su posterior habilitación judicial se le suma un tercer nivel de análisis que versa sobre la última etapa de estas herramientas, la cual es su utilización en un caso particular.

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

NIVEL III: USO OPERATIVO Y ADMINISTRATIVO DEL SPYWARE

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



NÚCLEO NORMATIVO

→ NIVEL III: USO OPERATIVO Y ADMINISTRATIVO DEL SPYWARE

En primer término es importante señalar que las técnicas intrusivas varían según el software utilizado, el dispositivo cuya vulnerabilidad será explotada y la casuística del caso concreto. Así las cosas, la medida habilitada por resolución judicial fundada puede llevarse a cabo de forma remota, en proximidad o mediante interacción física directa con el dispositivo, cada uno con sus particularidades pero siempre respetando un protocolo general. Por otro lado, las operaciones también varían considerablemente en complejidad y, por tanto, en su nivel de injerencia. En el extremo más básico, la autoridad puede descargar encubiertamente datos de un dispositivo móvil desatendido o utilizar credenciales de acceso para ingresar a información almacenada en una computadora. Las operaciones más complejas, que son posibles mediante spyware, implican necesariamente la explotación de vulnerabilidades existentes en el software para tomar control de dispositivos o redes, con el fin de extraer material de forma remota, monitorear al usuario del dispositivo o acceder a funciones del mismo.

No obstante, ante la ausencia de un protocolo marco en Argentina, estos protocolos suelen ser propios de cada fuerza de seguridad o de investigación, siendo los mismos opacos y con márgenes de discrecionalidad de difícil supervisión judicial. En este sentido, se nombrarán algunos aspectos que deberían tenerse en cuenta a la hora de establecer un Reglamento o Protocolo General de Uso para el empleo de estas herramientas.

La orden de autorización de la medida puede autorizar tanto la interferencia física —a saber, la descarga encubierta de datos de un dispositivo al que se ha accedido físicamente— como la interferencia remota, por ejemplo instalando un programa en un dispositivo a través de una red cableada o inalámbrica para extraer información de forma remota. Dadas las particularidades que pueden surgir en cada caso, sin perjuicio de los extensos recaudos que deben acreditarse de forma previa a la ejecución, puede suceder que en una operación se requieran conductas adicionales, que si bien no están expresamente detalladas en la orden son necesarias para ejecutar lo autorizado. En este caso, los diversos protocolos consultados suelen admitir estas conductas como “incidentales y necesarias”. Sin embargo,

cuando a través de estas conductas adicionales se obtengan datos de un dispositivo que no esté vinculado a la persona individualizada en la orden, la medida no tendrá lugar y deberá ordenarse el cese y borrado de los datos de ese dispositivo impropio que hayan sido obtenidos.

También es dable recordar que la medida deberá estar siempre sometida al doble test de necesidad y proporcionalidad, por tanto como se explicó anteriormente no podrá aplicarse si existen métodos menos intrusivos capaces de obtener la misma información. Asimismo, las personas de una autoridad habilitada para ordenar la medida, y quienes sean encargados de su uso o ejecución, deben recibir capacitación obligatoria y continua sobre sus responsabilidades profesionales y legales, incluyendo también actualizaciones de sus protocolos de seguridad particulares, que deben estar de acuerdo con el Reglamento General.

En cuanto a la trazabilidad de la actividad, las autoridades habilitadas deben tener la obligación de mantener registros detallados de todas las operaciones realizadas bajo el amparo de una orden de interceptación de comunicaciones. Estos registros deben documentar las solicitudes de interceptación, las autorizaciones otorgadas, las renovaciones y cancelaciones, las conductas incidentales, y cualquier error cometido en el curso de la operación. Esto es importante no solo por su naturaleza de control, sino también para que la medida ejecutada y los datos recolectados puedan gozar de la seguridad jurídica suficiente para poder ser utilizados como prueba ulteriormente en otros procesos posteriores si fuera necesario.

Es muy probable que debido al funcionamiento intrínseco a estas herramientas puedan verse vulnerados o reducidos derechos consagrados tanto en el plano nacional como internacional, tales como el respeto de la vida privada y familiar, la protección del domicilio y de la correspondencia en todas sus formas, la libertad de expresión, entre otros. En esta línea, también se considera una buena práctica que de forma previa a la ejecución de la medida en cuestión se evalúe explícitamente la intrusión colateral, es decir, la posible afectación a terceros no designados e individualizados en la orden. Esto posteriormente se complementa con el análisis de lo explicado ut supra, las llamadas "conductas incidentales". En los casos en que una conducta no sea claramente incidental, sino que pueda constituir el uso separado de otra potestad, puede considerarse que se excedió en su objeto y que es necesaria una autorización independiente.

En cuanto al tratamiento de datos, los protocolos comparados suelen establecer categorías de información con diferentes niveles de protección. El concepto de material protegido—que incluye información privada o amparada por el secreto profesional y el contenido de comunicaciones— está sujeto a salvaguardas reforzadas, especialmente en el contexto de operaciones de interferencia masiva. También es importante disponer de reglas específicas para el manejo de material confidencial, tanto de información sujeta a secreto profesional legal como datos médicos o sensibles. Para acceder a material de estas categorías, se suelen exigir estándares de justificación más elevados y acreditar el cumplimiento de las salvaguardas particulares para cada tipo de información.

En cuanto al ciclo de vida del material obtenido mediante herramientas intrusivas, la regla general es que los datos deben conservarse sólo durante el tiempo estrictamente necesario para los fines que justificaron la medida, mientras que la diseminación del material está restringida: solo puede compartirse con personas que lo necesiten para el cumplimiento de las funciones que justificaron la orden, y debe mantenerse en el mínimo imprescindible.

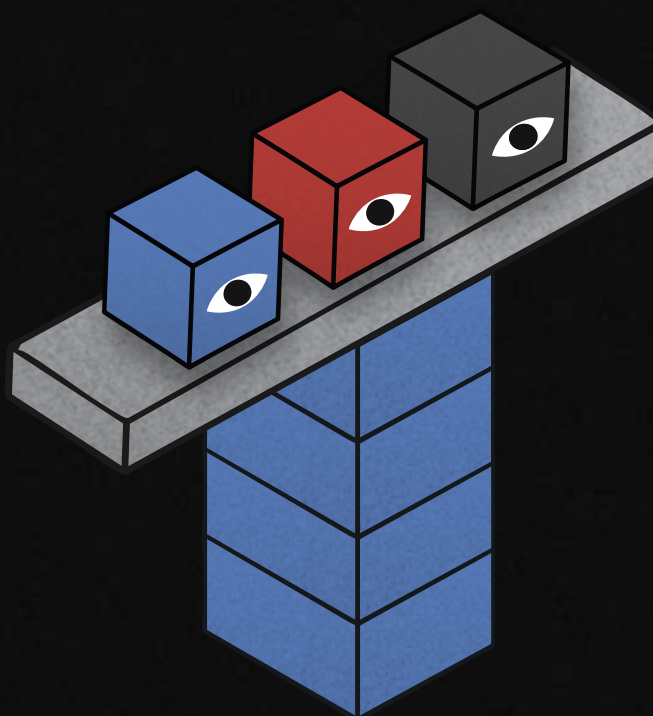
Respecto de la destrucción, justamente cuando el material deje de ser necesario para los fines autorizados, cuando la medida sea cancelada o nulificada, o cuando pase el plazo estipulado en el cuerpo legal correspondiente, debería procederse a su eliminación de forma segura. Si fuera necesario conservar algún dato recopilado, tiene que justificarse e informarse oportunamente.

Por último, en lo que respecta a la supervisión de la medida —más allá del arco legal—, el elevado nivel de riesgo que estas herramientas entrañan para los derechos fundamentales exige la designación de funcionarios específicamente responsables de verificar el cumplimiento de los procedimientos, revisar periódicamente las órdenes vigentes y reportar internamente cualquier error o desvío detectado. Dichos funcionarios deben contar con atribuciones de inspección, auditoría e investigación de posibles infracciones, así como también con la facultad de requerir información, acceder a las operaciones en curso y emitir informes públicos y recomendaciones orientadas a la actualización de los Protocolos Generales de Uso.

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

ARTICULACIÓN ENTRE NIVELES: HACIA UN SISTEMA INTEGRADO DE GOBERNANZA

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



ARTICULACIÓN ENTRE NIVELES: HACIA UN SISTEMA INTEGRADO DE GOBERNANZA

El análisis precedente ha puesto de manifiesto que el uso de spyware no puede ser comprendido ni regulado de manera adecuada si se lo aborda únicamente desde cada una de sus etapas por separado. La adquisición de la herramienta, su habilitación en el marco de un proceso judicial y su ejecución operativa no constituyen instancias autónomas, sino momentos interdependientes de un mismo proceso. Las decisiones que se adoptan en cada uno de estos niveles condicionan, de manera directa, el alcance y las consecuencias de las restantes.

Esta interdependencia implica que los riesgos asociados al uso de spyware no se originan únicamente en eventuales fallas de cada instancia considerada de forma aislada, sino en la desalineación entre ellas. Cuando los criterios que rigen la adquisición no dialogan con los estándares de habilitación judicial, o cuando las condiciones de autorización no se corresponden con las capacidades reales de la herramienta ni con los marcos que orientan su ejecución, el sistema en su conjunto pierde coherencia. En ese escenario, el control se vuelve fragmentario, la trazabilidad de las decisiones se diluye y los mecanismos de responsabilidad institucional se debilitan. En ausencia de una articulación efectiva, el sistema tiende a reproducir las fallas estructurales previamente identificadas, consolidando un esquema en el que el control formal pierde eficacia frente a la práctica efectiva de uso de estas herramientas.

En este sentido, la coherencia normativa no puede entenderse como la mera existencia de reglas en cada uno de los planos involucrados, sino como la capacidad de articularlas bajo criterios comunes que atraviesen la totalidad del ciclo de vida de la herramienta. Ello requiere que las condiciones bajo las cuales se adquiere un sistema de spyware sean compatibles con los estándares que rigen su habilitación y con las garantías que deben observarse en su uso efectivo. Esta articulación no sólo resulta necesaria para asegurar la consistencia del sistema, sino también para prevenir los riesgos asociados a usos indebidos, desviaciones funcionales o ampliaciones no autorizadas del alcance de la intervención. Sin esta correspondencia, incluso marcos regulatorios formalmente exigentes pueden resultar ineficaces frente a prácticas que, en los hechos, operan de manera descoordinada.

Sobre esta base, la construcción de un sistema integrado de gobernanza exige la definición de principios que orienten la articulación entre niveles. En primer lugar, la unidad de estándares, en tanto las exigencias aplicables a la utilización de estas herramientas deben ser coherentes desde su adquisición hasta su ejecución. En segundo lugar, la continuidad del control, que supone la existencia de mecanismos de supervisión que no se agoten en el momento de la autorización judicial, sino que acompañen la implementación de la medida en todas sus etapas. En tercer lugar, la trazabilidad de las decisiones, como condición necesaria para reconstruir el recorrido completo de la herramienta y verificar el cumplimiento de los límites establecidos. Finalmente, la visibilidad del sistema en su conjunto, en la medida en que la opacidad estructural de estas tecnologías no puede traducirse en opacidad institucional.

Estos principios deben traducirse en arreglos institucionales que permitan materializar la integración entre niveles. En particular, resulta necesario prever instancias de validación técnica que acompañen la toma de decisiones en los distintos momentos del proceso, así como mecanismos de registro y documentación que aseguren la trazabilidad del ciclo completo de implementación. Del mismo modo, la previsión de esquemas de supervisión continua y de control independiente contribuye a reducir los márgenes de opacidad y discrecionalidad que caracterizan a estas prácticas. Estos aspectos serán desarrollados en detalle en los capítulos siguientes.

La articulación entre niveles no constituye únicamente una mejora organizativa, sino una condición necesaria para que los límites jurídicos establecidos puedan operar de manera efectiva en la práctica. En este marco, dicha articulación se presenta como una condición de eficacia de las garantías que rigen la medida y, en última instancia, como un presupuesto para su validez en términos de control sustantivo. En ausencia de esta articulación, el uso de spyware queda, en los hechos, condicionado por la capacidad técnica y operativa de quienes lo implementan, antes que por los límites formales establecidos por el derecho. En este sentido, la gobernanza integrada no solo cumple una función de ordenamiento institucional, sino también de mitigación de riesgos en sistemas cuyo potencial de afectación excede los supuestos tradicionales de control.

A ello se suma un elemento adicional que debe ser considerado en el diseño de estos mecanismos. La aptitud de estas herramientas para operar sobre comunicaciones y sistemas digitales que, por su propia naturaleza, pueden

involucrar flujos de información que exceden los límites de una jurisdicción específica introduce una tensión entre la escala territorial del derecho penal y la escala real de las tecnologías de intervención. Aun cuando su utilización en casos concretos pueda circunscribirse a un ámbito territorial determinado, esta capacidad estructural constituye un fundamento relevante para la incorporación de instancias de coordinación y validación a nivel federal.

En este sentido, la previsión de mecanismos de validación a nivel federal para el despliegue de estas herramientas por parte de jurisdicciones locales constituye una alternativa institucionalmente relevante. Bajo este esquema, la decisión de solicitar la medida permanecería en cabeza de los órganos judiciales locales, pero su implementación efectiva requeriría la intervención de una instancia federal con capacidades técnicas especializadas, orientada a verificar el cumplimiento de estándares homogéneos en materia de alcance, proporcionalidad, configuración técnica y condiciones de uso de la herramienta. Esta intervención se configura como una instancia de validación técnica y de control concurrente, sin alterar la titularidad de la competencia jurisdiccional ni el alcance de la decisión judicial local. De este modo, se incorpora una capa adicional de control que permite alinear la dimensión jurídica de la medida con sus implicancias técnicas y su potencial alcance interjurisdiccional.

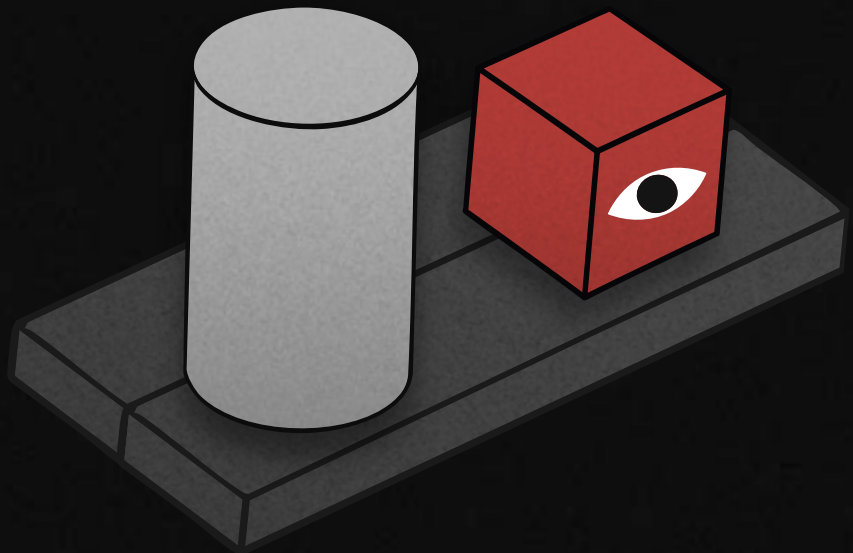
Estos mecanismos no reemplazan la necesidad de una gobernanza integrada, pero constituyen un recurso relevante para alinear las escalas institucionales con las capacidades técnicas de estas herramientas y reducir los niveles de fragmentación en su implementación.

En última instancia, la regulación del spyware no puede limitarse a establecer condiciones de uso en abstracto ni a reforzar de manera aislada los requisitos de autorización judicial. Además, requiere concebir la intervención estatal sobre dispositivos digitales como un proceso integrado, cuya legitimidad depende tanto de las decisiones que habilitan su uso como de las condiciones bajo las cuales esas decisiones son implementadas y controladas. Sin esta mirada sistémica, el derecho corre el riesgo de regular fragmentos de un fenómeno cuya lógica de funcionamiento es, por definición, transversal y excede los marcos tradicionales de regulación segmentada.

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

RECOMENDACIONES

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



RECOMENDACIONES

→ LINEAMIENTOS DE POLÍTICA PÚBLICA

Como se ha desarrollado a lo largo del presente documento, el principal desafío que plantea la incorporación estatal de herramientas de spyware no radica únicamente en su capacidad intrusiva, sino en la ausencia de mecanismos institucionales capaces de gobernar de manera coherente su ciclo completo de vida. La adquisición de estas tecnologías, su habilitación judicial y su utilización operativa suelen encontrarse sujetas a regímenes normativos diferenciados, administrados por actores distintos y bajo lógicas institucionales que no siempre se encuentran alineadas. En consecuencia, la política pública en esta materia no debería orientarse exclusivamente a regular cada etapa de manera aislada, sino a asegurar que las decisiones adoptadas en cada una de ellas respondan a criterios compatibles entre sí y puedan ser sometidas a mecanismos efectivos de control y rendición de cuentas.

En este contexto, resulta importante comprender que la adquisición de spyware no implica únicamente la compra de una herramienta informática. Lo que el Estado incorpora en estos casos son capacidades extraordinarias de vigilancia e intrusión que permiten acceder de manera remota y encubierta a dispositivos, comunicaciones y datos personales. Por esa razón, las decisiones relativas a su adquisición, autorización y utilización no pueden ser tratadas como cuestiones puramente técnicas o administrativas, sino como decisiones institucionales capaces de alterar de manera significativa el equilibrio entre las necesidades de investigación y la protección de los derechos fundamentales.

La experiencia comparada demuestra que una parte importante de los riesgos asociados a estas tecnologías aparece cuando la decisión de utilizarlas, su implementación técnica y su control posterior quedan concentrados dentro de una misma estructura institucional. En esos escenarios, los mecanismos de supervisión tienden a debilitarse, la trazabilidad de las decisiones se vuelve más difícil y aumenta la dependencia respecto de quienes poseen el conocimiento técnico necesario para operar estas herramientas. En consecuencia, las políticas públicas orientadas a regular el spyware deberían promover esquemas que distribuyan funciones de autorización, ejecución,

validación técnica y supervisión entre distintos actores estatales, evitando que una misma autoridad concentre la totalidad del proceso.

Esta cuestión adquiere particular relevancia en sistemas federales como el argentino. A lo largo de este documento se ha señalado que la distribución de competencias entre jurisdicciones puede favorecer la fragmentación regulatoria, la coexistencia de estándares heterogéneos y las dificultades de coordinación. Sin embargo, esas mismas características pueden convertirse en una herramienta útil para fortalecer los mecanismos de control. El federalismo no sólo distribuye competencias: también distribuye poder. En consecuencia, la intervención coordinada de órganos pertenecientes a distintos niveles de gobierno puede contribuir a generar controles cruzados que reduzcan los riesgos asociados a la concentración de capacidades intrusivas en un único actor institucional.

Desde esta perspectiva, la respuesta frente a los desafíos que plantea el spyware no debería limitarse a la fijación de estándares mínimos comunes para todas las jurisdicciones. También debería promover mecanismos de cooperación y control que permitan que distintas autoridades participen de las etapas más sensibles del proceso. La magnitud de la intrusión que estas herramientas permiten aconseja explorar modelos en los cuales la autorización judicial, la validación técnica de la medida, su ejecución operativa y su supervisión posterior no dependan exclusivamente de una única institución, sino que puedan incorporar instancias adicionales de control y revisión. Este tipo de soluciones resulta especialmente relevante cuando las medidas proyectan sus efectos sobre sistemas de comunicación o flujos de información que, por su propia naturaleza, exceden los límites territoriales de una jurisdicción determinada.

Asimismo, cualquier estrategia regulatoria seria debe contemplar el fortalecimiento de las capacidades institucionales de control. La eficacia de las salvaguardas jurídicas no depende únicamente de las competencias formales atribuidas a jueces, organismos de control o autoridades administrativas, sino también de su capacidad efectiva para comprender, auditar y cuestionar el funcionamiento de estas tecnologías. La incorporación de capacidades estatales de vigilancia sin el desarrollo paralelo de capacidades técnicas de supervisión genera una asimetría estructural que termina debilitando la efectividad de los controles previstos por el propio ordenamiento jurídico.

En definitiva, la política pública en materia de spyware debería orientarse

hacia un modelo de prevención estructural. Ello supone actuar sobre las condiciones institucionales que posibilitan o amplifican los riesgos asociados a estas herramientas antes de que los abusos se produzcan. En contextos como el argentino, caracterizados por una distribución compleja de competencias y por capacidades técnicas desiguales entre jurisdicciones, la construcción de controles cruzados, mecanismos de coordinación y capacidades efectivas de supervisión constituye una condición necesaria para que cualquier regulación alcance niveles razonables de eficacia, legitimidad democrática y protección de derechos fundamentales.

→ RECOMENDACIONES ESPECÍFICAS

Las pautas de política pública enunciadas en el apartado anterior definen el marco general de coordinación federal, pero su eficacia depende de que se logren traducir en exigencias concretas y verificables en cada uno de los planos identificados a lo largo de esta exposición. En tal sentido, a continuación se desarrollan recomendaciones específicas para cada etapa del ciclo de vida completo del spyware —adquisición, habilitación judicial, uso operativo, obtención y destrucción, todo ello sujeto a supervisión integral—, con el propósito de que la coherencia normativa postulada como principio rector no quede librada a una mera declaración de intenciones, sino que se sostenga en mecanismos institucionales concretos y exigibles en la práctica.

- **ADQUISICIÓN: IDONEIDAD TÉCNICA E IDONEIDAD PROBATORIA DE LA HERRAMIENTA**

Los pliegos de contratación de herramientas de intrusión deben exigir, como condición de admisibilidad de la oferta, que el proveedor acredite: (i) capacidad de generar registros de auditoría inalterables de cada despliegue, exportables a un sistema de control ajeno al propio proveedor; (ii) limitación técnica configurable del alcance de captación por orden judicial individual, de modo que la herramienta no permita por defecto una recolección más amplia que la autorizada; y (iii) la inexistencia de cláusulas de confidencialidad que impidan al Estado contratante someter el funcionamiento del software

a auditorías técnicas independientes, aun cuando estas se desarrollen bajo reserva y acuerdos de confidencialidad.

Asimismo, la evaluación previa a la contratación no debe limitarse a las capacidades operativas de la herramienta, sino extenderse a su aptitud para producir información susceptible de ser utilizada como evidencia en un proceso judicial. A tal fin, deberá acreditarse que el sistema permite documentar adecuadamente las operaciones realizadas, preservar la integridad de la información obtenida, reconstruir la secuencia de actuaciones ejecutadas y someter sus resultados a mecanismos posteriores de auditoría, control judicial y contradicción procesal.

La adquisición de herramientas cuya arquitectura técnica impida verificar de manera independiente el origen, alcance o integridad de la información obtenida resulta incompatible con las exigencias propias de producción y valoración de la prueba en un Estado de Derecho. En consecuencia, la ausencia de garantías mínimas de trazabilidad, auditabilidad e integridad probatoria debe constituir una causal suficiente para descartar su contratación por parte del Estado.

Un antecedente reciente que ilustra la viabilidad de esta exigencia es la *Secure by Demand Guide*⁵, publicada conjuntamente por la Agencia de Ciberseguridad e Infraestructura (CISA) y el FBI de los Estados Unidos en 2024, sumado a posteriores actualizaciones. La guía introduce un catálogo estandarizado de preguntas técnicas que los organismos gubernamentales deben dirigir a los proveedores de software como condición previa a la contratación, abarcando desde la acreditación de prácticas de desarrollo seguro hasta la provisión de un inventario verificable de componentes (*software bill of materials*) y la documentación de controles sobre la cadena de suministro. Aunque no fue diseñada específicamente para herramientas de intrusión, su arquitectura regulatoria es directamente trasladable debido a que demuestra que es técnicamente posible y jurídicamente practicable convertir exigencias de seguridad y auditabilidad en criterios de admisibilidad de la oferta, de forma previa a cualquier evaluación de mérito o precio. Aplicada al ámbito del spyware, esa lógica equivale a exigir que el proveedor

5 <https://www.cisa.gov/resources-tools/resources/secure-demand-priority-considerations-operational-technology-owners-and-operators-when-selecting>

acredite, antes de que el Estado decida si contrata, que la herramienta es técnicamente apta para ser compatible con los principios de nuestro Estado Nacional y su legislación interna.

- **HABILITACIÓN JUDICIAL: VALIDACIÓN TÉCNICA PREVIA A LA EJECUCIÓN**

La autorización judicial de medidas que impliquen el despliegue de herramientas de spyware debe complementarse con una instancia de validación técnica previa a su ejecución. A diferencia de otras medidas de investigación tradicionales, la complejidad técnica de estas herramientas impide asumir que la configuración efectivamente utilizada durante el despliegue coincidirá necesariamente con los términos establecidos en la resolución judicial que la autoriza.

Por ello, con carácter previo a la ejecución de la medida, debería intervenir una unidad técnica distinta de la autoridad requirente y de la fuerza encargada de su despliegue, cuya función consista en verificar que los parámetros de configuración de la herramienta se ajustan a las condiciones establecidas en la resolución judicial. Esta verificación deberá comprender, como mínimo, la identidad de los dispositivos afectados, las funcionalidades habilitadas, el alcance de la captación autorizada, el plazo de ejecución y cualquier otra limitación expresamente impuesta por el magistrado. El resultado de esta intervención deberá documentarse mediante acta o informe técnico incorporado al expediente.

Asimismo, dado que estas medidas pueden desplegarse sobre dispositivos, comunicaciones y sistemas informáticos cuyos efectos exceden materialmente los límites territoriales de una única jurisdicción, resulta conveniente que esta instancia de validación sea ejercida por un órgano federal especializado. Esta intervención no tiene por objeto revisar la procedencia de la medida ni sustituir el control jurisdiccional ejercido por el magistrado competente, sino aportar una instancia adicional de verificación técnica respecto de herramientas cuya ejecución puede proyectar efectos más allá del ámbito territorial de la autoridad que las solicita. Su participación contribuye, además, a promover criterios homogéneos de implementación, reducir las asimetrías técnicas existentes entre jurisdicciones y fortalecer la

trazabilidad de las actuaciones.

La existencia de esta instancia de validación fortalece la correspondencia entre la medida autorizada y la efectivamente ejecutada, reduce el riesgo de desviaciones durante su implementación y proporciona mayores garantías respecto del alcance real de la intervención realizada.

Un antecedente institucional que permite visualizar la viabilidad de este mecanismo de validación técnica previa a la ejecución es la *Toetsingscommissie Inzet Bevoegdheden*⁶ (TIB), creada por la Ley de Servicios de Inteligencia y Seguridad neerlandesa en el año 2017. Esta TIB revisa con carácter previo y vinculante la legalidad de las autorizaciones ministeriales para el ejercicio de poderes especiales de inteligencia y está integrada de forma mixta por tres miembros: al menos dos de ellos con trayectoria judicial y al menos uno que haya sido designado en razón de su competencia técnica especializada. Esta composición le permite al TIB evaluar no solo la adecuación jurídica de la medida sino también si los medios técnicos concretos se corresponden con lo autorizado. En su primer período de funcionamiento la TIB rechazó aproximadamente el 5% de las solicitudes revisadas, lo que demuestra que el control ex ante con competencia técnica es viable y no opera como una instancia de mera ratificación formal.

- EJECUCIÓN: TRATAMIENTO DIFERENCIADO DE MATERIAL AMPARADO POR SECRETO PROFESIONAL

Cuando durante la ejecución de una medida de spyware se advierta la existencia de comunicaciones, documentos o información que pudiera encontrarse amparada por un deber de secreto profesional o un régimen especial de confidencialidad, deberá suspenderse inmediatamente su revisión y aplicarse un procedimiento específico de resguardo.

A estos efectos, se considerará especialmente protegida la información

⁶ <https://english.aivd.nl/about-aivd/the-intelligence-and-security-services-act-2017/regulatory-commission>

vinculada al ejercicio de la defensa en juicio, al secreto profesional abogado-cliente, a la protección de fuentes periodísticas y a la información médica o sanitaria, sin perjuicio de otras categorías que puedan encontrarse amparadas por regímenes legales específicos.

La identificación de material perteneciente a alguna de estas categorías deberá ser comunicada de inmediato al magistrado interviniente, limitándose dicha comunicación a informar su existencia y características generales, sin avanzar sobre el contenido protegido. Hasta tanto se adopte una decisión judicial específica, el material deberá permanecer aislado en un repositorio de acceso restringido y no podrá ser objeto de análisis, extracción, copia, utilización operativa ni incorporación al proceso. Tampoco podrá servir de fundamento para la adopción de nuevas medidas de investigación mientras no exista autorización judicial expresa para su revisión.

La autorización de acceso al dispositivo no implica, por sí sola, autorización para revisar material alcanzado por regímenes especiales de confidencialidad. El acceso a esta información requerirá una decisión judicial autónoma y específicamente fundada respecto del material cuya revisión se pretende autorizar, las razones que justifican su examen y el alcance concreto de la habilitación otorgada.

Asimismo, cuando la medida recaiga sobre personas respecto de las cuales resulte razonablemente previsible la existencia de información protegida por deberes especiales de confidencialidad —tales como abogados, periodistas, profesionales de la salud u otros sujetos alcanzados por obligaciones legales de secreto profesional— la resolución judicial deberá contener una fundamentación reforzada respecto de la necesidad de la medida, la imposibilidad de obtener la información perseguida mediante medios menos intrusivos, los riesgos asociados a la captación de material protegido y las salvaguardas previstas para minimizar su afectación.

En estos supuestos, dicha fundamentación deberá ser sometida a la instancia de validación técnica prevista en el apartado anterior, la cual verificará que la configuración de la herramienta incorpora efectivamente las restricciones, limitaciones y mecanismos de resguardo establecidos por el magistrado. La finalidad de esta revisión no consiste en sustituir la decisión jurisdiccional, sino en asegurar que las salvaguardas dispuestas por el juez puedan traducirse efectivamente en parámetros técnicos verificables durante la

ejecución de la medida.

La existencia de un procedimiento diferenciado para este tipo de información permite compatibilizar las necesidades legítimas de investigación con la preservación de ámbitos de confidencialidad cuya protección resulta indispensable para el adecuado ejercicio del derecho de defensa, la actividad periodística, el secreto profesional y otros intereses especialmente tutelados por el ordenamiento jurídico.

El tratamiento distintivo de material específicamente protegido encuentra respaldo en la experiencia comparada, más precisamente con lo consagrado en el *Equipment Interference Code of Practice*⁷ del Reino Unido. Este Código de Prácticas para la Interferencia de Dispositivos establece categorías expresas de material especialmente protegido, ya sea por tratarse de comunicaciones amparadas por privilegio legal, de comunicaciones entre un parlamentario y otra persona en ejercicio de su mandato, o por ser relativo a información personal confidencial o al material periodístico confidencial. En este caso, la información personal confidencial abarca específicamente la información mantenida en reserva acerca de una persona, viva o fallecida, que resulte identificable a partir de ella, cuando el material se refiera a su salud física o mental o a consultas espirituales, incluyendo tanto comunicaciones orales como escritas.

Si la medida puede comprometer alguna de esas categorías, requerirá una carga adicional de justificación en la solicitud de habilitación. Cuando el propósito de la orden es autorizar la interceptación de comunicaciones que el solicitante cree que contendrán material periodístico confidencial, o bien identificar o confirmar la fuente de información periodística, la solicitud debe incluir una declaración a ese efecto y detallar los arreglos previstos para el manejo, la retención, el uso y la destrucción de ese material. Asimismo, el Código también establece una regla de no utilización del material protegido cuando se exceda del marco del proceso en curso.

7 <https://www.gov.uk/government/publications/investigatory-powers-act-draft-codes-of-practice-march-2025>

- RETENCIÓN Y DESTRUCCIÓN: REVISIÓN PERIÓDICA DE UTILIDAD PROCESAL

La autorización judicial de una medida de spyware no habilita, por sí sola, la conservación indefinida de la información obtenida. Una vez finalizada la medida, corresponderá al magistrado interviniente verificar periódicamente si el material recolectado continúa siendo necesario para la investigación o para los fines probatorios del proceso.

La conservación de dicha información deberá encontrarse expresamente fundada en su utilidad procesal actual. La mera posibilidad de una utilidad futura o eventual no constituirá fundamento suficiente para mantener su retención.

Cuando desaparezca el interés procesal que justificó su conservación, deberá ordenarse su destrucción o eliminación definitiva. Dicha operación deberá documentarse mediante acta o certificación técnica incorporada al expediente, en la que consten la identificación del material eliminado, la fecha de la operación, el procedimiento empleado y el funcionario responsable de su ejecución. La viabilidad operativa de este mecanismo encuentra respaldo parcial en el régimen del Título III del *Omnibus Crime Control and Safe Streets Act*⁸ estadounidense. Esta normativa somete a revisión judicial la necesidad de retener la información obtenida luego del cese de la medida; al mismo tiempo que consagra una exclusión probatoria del material que no haya cumplido con los criterios y estándares legales de obtención. El referido cuerpo legal establece que toda orden de interceptación debe terminar al alcanzar el objetivo autorizado, sin aguardar el vencimiento del plazo máximo; y también articula el mecanismo de contralor, en tanto faculta al juez para exigir informes periódicos de progreso que acrediten la subsistencia de la necesidad de continuar la medida. De este modo, la conservación del material perderá su fundamento procesal en cuanto ese objetivo haya sido alcanzado.

Sin perjuicio de ello, creemos conveniente adicionar como corolario de esta recomendación particular que ante la ausencia de documentación o certificación técnica que permita acreditar la destrucción de la información obtenida, esto impedirá tener por cumplida la orden de destrucción y obstará a cualquier invocación posterior de dicho material como elemento de prueba.

- SUPERVISIÓN: INFORME ANUAL DE IMPLEMENTACIÓN Y CONTROL

El órgano responsable de la supervisión del Reglamento o Protocolo General de Uso deberá elaborar, con periodicidad anual, un informe consolidado sobre la utilización de herramientas de spyware en las distintas jurisdicciones alcanzadas por el régimen. Dicho informe deberá contener, como mínimo, información agregada relativa a la cantidad de medidas solicitadas, autorizadas, rechazadas, prorrogadas y finalizadas; la duración promedio de las intervenciones; la cantidad de incidentes o desvíos detectados durante su implementación; los resultados de las actividades de supervisión realizadas; y las recomendaciones normativas, técnicas u operativas que resulten pertinentes para mejorar el funcionamiento del sistema. En ningún caso la información publicada podrá permitir la identificación de causas, personas investigadas o datos protegidos por reserva legal.

La finalidad de este mecanismo no consiste únicamente en dotar de publicidad a la utilización de estas herramientas, sino también en generar información que permita evaluar su funcionamiento, identificar problemas recurrentes de implementación, detectar asimetrías entre jurisdicciones y promover la actualización continua de los estándares de control aplicables. Las facultades estatales de investigación más intrusivas requieren mecanismos de rendición de cuentas que permitan conocer su utilización de manera agregada y sistemática. La opacidad técnica inherente a este tipo de tecnologías no debe traducirse en opacidad institucional respecto de su empleo, alcance y frecuencia de utilización. En tal sentido, la elaboración periódica de información consolidada constituye una herramienta indispensable para dotar de visibilidad al funcionamiento general del sistema, fortalecer los mecanismos de supervisión existentes y facilitar el debate informado sobre su utilización.

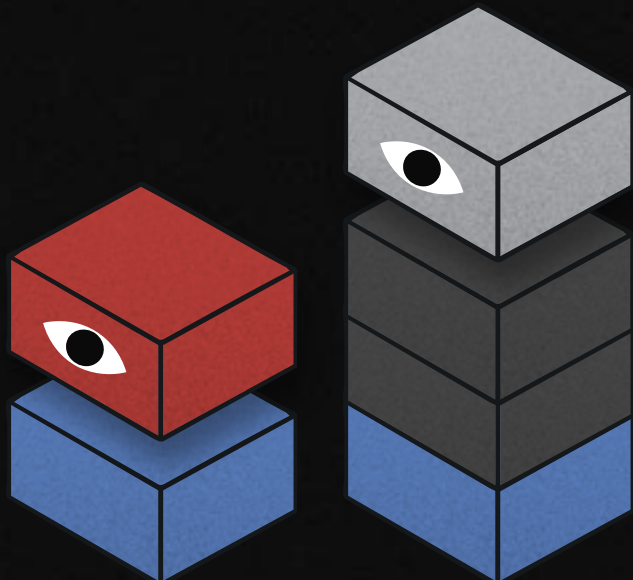
Un antecedente relevante de este tipo de mecanismos puede encontrarse en los *Wiretap Reports*⁹ elaborados anualmente por la *Administrative Office of the United States Courts* en cumplimiento de 18 U.S.C. § 2519. Estos informes consolidan información estadística sobre las órdenes de interceptación de comunicaciones autorizadas por tribunales federales y estatales, incluyendo cantidad de medidas, duración, delitos investigados y resultados obtenidos. Si bien se trata de una herramienta concebida para supervisar interceptaciones de comunicaciones y no medidas de spyware, su experiencia demuestra la viabilidad de producir información pública agregada sobre facultades estatales especialmente intrusivas sin comprometer la reserva de investigaciones concretas.

9 <https://www.uscourts.gov/data-news/reports/statistical-reports/wiretap-reports>

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

CONCLUSIONES

0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0



CONCLUSIONES

A lo largo de este trabajo se ha procurado demostrar que el spyware no constituye simplemente una herramienta tecnológica más en el repertorio investigativo estatal, sino que instituye una categoría jurídica y política radicalmente nueva que desafía los presupuestos sobre los que se ha asentado la regulación procesal tradicional. El análisis desarrollado permite afirmar que la capacidad de intrusión que estas herramientas confieren al Estado no es comparable —ni gradualmente ni por analogía— con las técnicas de interceptación que el derecho conoce y que ha procurado regular desde el constitucionalismo moderno. En este sentido, la diferencia no es meramente cuantitativa, ya que no se trata de que el spyware permita acceder a más información que una interceptación telefónica, sino de que accede a una dimensión cualitativamente distinta de la vida privada de una persona. Este acceso integral a su entorno digital, de forma subrepticia y persistente, acaba por redefinir estructuralmente la relación entre el poder estatal y los derechos fundamentales sometidos a su alcance.

En definitiva, esta constatación impone una consecuencia metodológica ineludible, en tanto las garantías actuales existentes en el ordenamiento procesal no pueden trasladarse a este nuevo ámbito mediante una mera aplicación analógica. Los estándares de autorización diseñados para la interceptación de comunicaciones, pensados tradicionalmente para una intervención acotada, pasiva y temporalmente definida, no resultan suficientes frente a una herramienta cuya naturaleza técnica es activa, potencialmente ilimitada y estructuralmente opaca. Aplicarlos de manera directa no implica extender las garantías al nuevo contexto, sino paradójicamente vaciarlas de contenido al intentar imponerlas a una realidad para la que no fueron concebidas. En este sentido, el desafío regulatorio que plantea el spyware no es el de adaptar normas existentes, sino el de construir un nuevo marco propio que parta del reconocimiento de su singularidad técnica y de sus consecuencias jurídicas específicas.

Por otra parte, se expuso claramente que los riesgos del spyware no se agotan en la dimensión técnica de la herramienta ni en las condiciones bajo las cuales puede ser autorizada judicialmente, sino que estos se proyectan sobre la totalidad del ciclo de vida del software. Este ciclo se compone partiendo de las decisiones que determinan qué capacidades incorpora el Estado, pasando por los criterios que habilitan su despliegue en un proceso

particular, y llegando hasta los protocolos que regulan su ejecución efectiva y el destino final de la información obtenida. La fragmentación de este ciclo en instancias separadas, gobernadas por actores distintos bajo lógicas institucionales descoordinadas, representa el factor principal a través del cual los riesgos inherentes a estas herramientas se materializan y amplifican. Sin articulación entre niveles, los marcos normativos más exigentes tienden a operar como garantías formales desprovistas de eficacia sustantiva.

Asimismo, esta problemática adquiere una dimensión adicional en contextos federales. La distribución de competencias entre el nivel nacional y los niveles subnacionales termina siendo una variable que contribuye y acrecienta el problema regulatorio. En un sistema como el argentino, donde la potestad procesal es predominantemente provincial y donde los regímenes de contratación, las estructuras de seguridad y las capacidades técnicas se distribuyen de manera dispar entre jurisdicciones, la ausencia de mecanismos de coordinación y estándares comunes termina produciendo condiciones estructurales que favorecen los desvíos de uso, la fragmentación del control y la concentración de capacidades de vigilancia al margen de los mecanismos institucionales de supervisión. En este contexto, el federalismo debe ser un elemento a incorporar en el diseño mismo del mecanismo de gobernanza integral postulado.

En suma, las recomendaciones específicas desarrolladas en la parte final de este trabajo intentan traducir estos principios de gobernanza integral en exigencias institucionales concretas, organizadas justamente en torno al ciclo completo de vida del spyware. Propuestas como la acreditación de condiciones técnicas de auditabilidad como criterio de admisibilidad en la contratación, la validación técnica previa a la ejecución como complemento indispensable de la autorización judicial, el tratamiento diferenciado del material amparado por secreto profesional, los mecanismos de destrucción documentalmente verificables y la obligación de publicar informes periódicos de implementación no constituyen recomendaciones aisladas, sino componentes de un sistema cuya racionalidad se asienta en la articulación mutua. La experiencia comparada en andamiajes jurídicos como el de los Países Bajos o el Reino Unido demuestra que estos mecanismos son viables institucional y jurídicamente, y que su adopción no compromete en forma alguna la eficacia investigativa estatal. De hecho, lejos de arriesgarla, acaba por enmarcarla en condiciones de legitimidad democrática que en el ordenamiento argentino actual se encuentran pendientes de construcción.

Finalmente, sostenemos que la incorporación de herramientas de alta intrusión como el spyware al aparato investigativo estatal no representa un fenómeno reversible. Por el contrario, las capacidades que el Estado adquiere raramente son abandonadas de manera voluntaria, y si a esto se le suma la presión por mantener efectividad frente a entornos tecnológicos crecientemente complejos se torna improbable cualquier retroceso orientado más a una prohibición o restricción de uso. El debate, por tanto, no puede plantearse en términos de si el Estado debe o no disponer de estas herramientas, sino en términos de bajo qué condiciones institucionales, con qué límites normativos y a través de qué mecanismos de control y rendición de cuentas puede hacerlo de manera compatible con los compromisos fundamentales del Estado de Derecho. Responder seriamente a esa pregunta es la tarea que este trabajo ha procurado iniciar, con la convicción de que la construcción de un marco regulatorio integral adecuado para el spyware constituye una exigencia ineludible para mantener la plena vigencia del orden constitucional y las garantías sobre las que se sustenta la totalidad de nuestro ordenamiento jurídico nacional.

