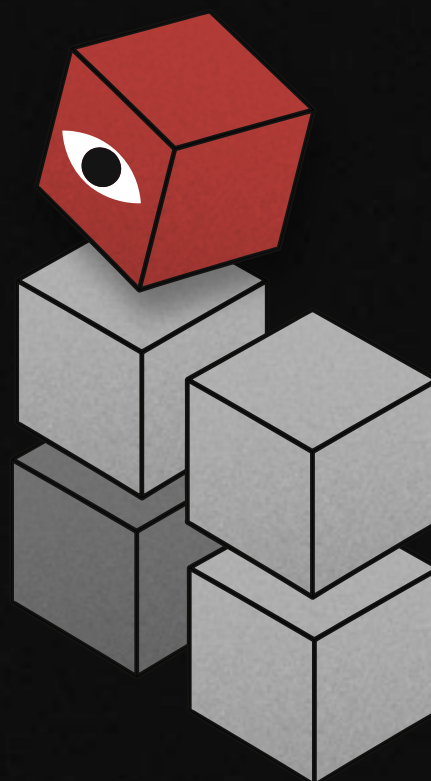


0 1 0 1 0 1  
1 0 1 0 1 0  
0 1 0 1 0 1  
1 0 1 0 1 0  
0 1 0 1 0 1  
1 0 1 0 1 0  
0 1 0 1 0 1  
1 0 1 0 1 0

# /SPYWARE: USO JUDICIAL EN ARGENTINA

SITUACIÓN NORMATIVA Y DE IMPLEMENTACIÓN  
EN LAS DISTINTAS JURISDICCIONES

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: uso judicial en Argentina.  
Situación normativa y de implementación  
en las distintas jurisdicciones"**

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

Versión preliminar. Documento en desarrollo.

Buenos Aires, junio de 2026  
Realizado con el apoyo de Spyware Accountability  
Initiative (SAI)

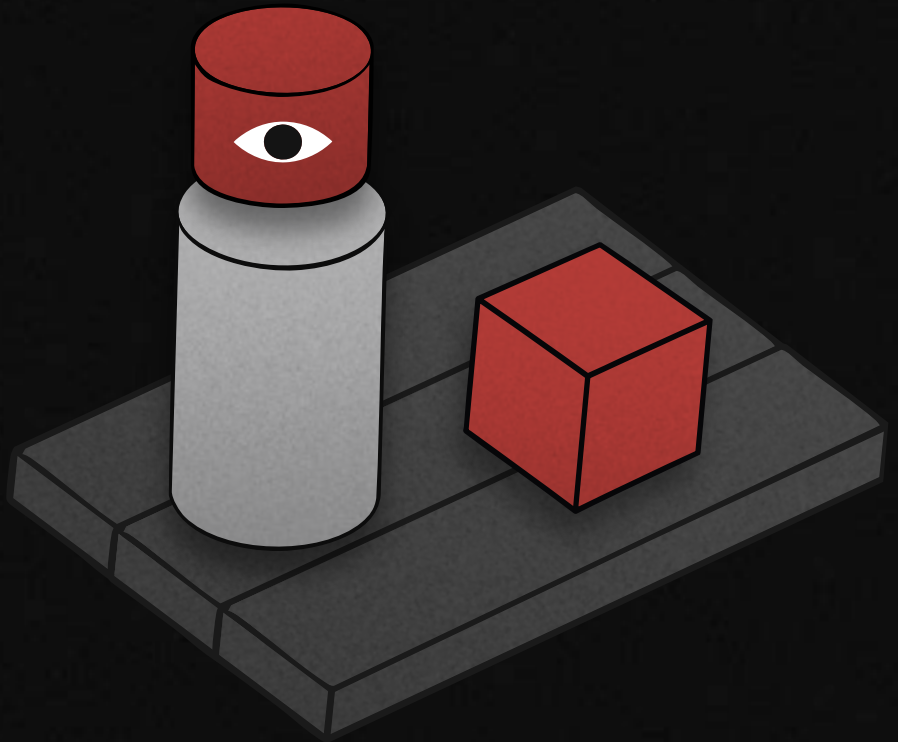
# ÍNDICE

|    |                                                                              |
|----|------------------------------------------------------------------------------|
| 3  | Introducción                                                                 |
| 5  | Marcos normativos e implementación                                           |
| 6  | Marco conceptual y estándares de referencia                                  |
| 7  | El análisis normativo de las 25 jurisdicciones<br>Niveles de riesgo          |
| 11 | El nivel de implementación real: resultados de los<br>pedidos de información |
| 14 | Conclusiones y hallazgos transversales                                       |
| 18 | ANEXO: Análisis normativo por jurisdicción                                   |

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

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

Este informe analiza el marco normativo aplicable al uso de software espía (*spyware*) en el proceso penal argentino, tanto en función de los códigos procesales penales provinciales como a nivel federal. Por un lado, examina las disposiciones que regulan (o que podrían habilitar) la interceptación de comunicaciones y el allanamiento remoto de dispositivos digitales por parte del Poder Judicial y el Ministerio Público Fiscal; y, por otro, presenta información sobre el nivel de implementación real en cada jurisdicción recabada a través de pedidos de información pública cursados a las respectivas jurisdicciones.

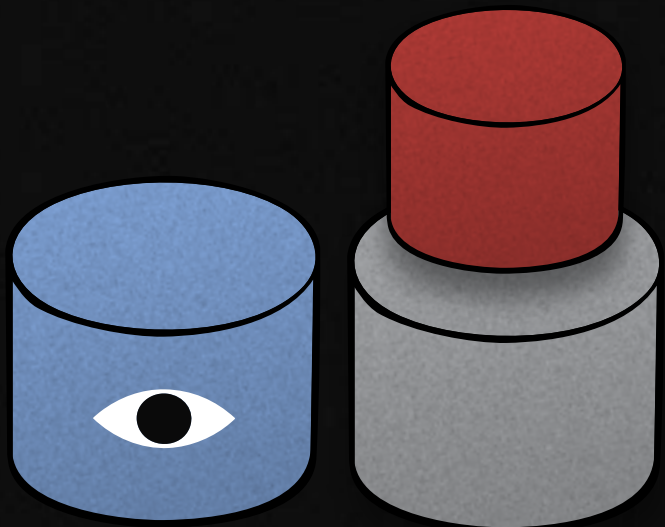
La información solicitada fue distinta según si la regulación de fondo provincial habilita expresamente el uso de *spyware* en el marco de una investigación penal, si lo prohíbe o si lo regula de manera abstracta, vaga o de una forma que podría indicar una habilitación bajo cierta interpretación. De esta forma y según el caso, consultamos específicamente si las autoridades judiciales consideran que existe una interpretación institucional que habilite el uso de herramientas intrusivas, si se adquirió software de este tipo y si existen protocolos o guías de uso al respecto.

Es importante advertir que la mayoría de las jurisdicciones no respondió las solicitudes, o no lo hizo de forma acabada. Además del vacío de información que implica, esta ausencia de respuesta completa constituye, en sí misma, un indicador político relevante, en tanto revela una opacidad estructural en torno a la regulación y uso de herramientas de vigilancia digital por parte del Estado, siendo éste un campo especialmente sensible para los derechos fundamentales.

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

# MARCOS NORMATIVOS E IMPLEMENTACIÓN

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



## MARCOS NORMATIVOS E IMPLEMENTACIÓN

### → MARCO CONCEPTUAL Y ESTÁNDARES DE REFERENCIA

El *spyware* es una categoría de herramienta informática que permite, entre otras cosas, acceder de forma remota y encubierta a dispositivos digitales (teléfonos, computadoras, tablets) para extraer información, monitorear comunicaciones en tiempo real, acceder a conversaciones previas, activar micrófonos o cámaras, y rastrear la ubicación de las personas sin su conocimiento. En el contexto de la investigación penal, su uso supone una medida de gran injerencia en la intimidad y la privacidad de las personas, que va mucho más allá de la interceptación tradicional de comunicaciones telefónicas.

En el ordenamiento procesal penal, dos figuras normativas resultan especialmente relevantes para el uso de *spyware*: la interceptación de comunicaciones, entendida como el acceso al contenido de las comunicaciones de la persona investigada (en vivo o con posterioridad); y el allanamiento remoto, que implica el ingreso encubierto a un dispositivo o sistema informático para obtener datos o activar funciones del equipo.

Mientras que la interceptación tiene tradición legislativa en todos los códigos analizados, el allanamiento remoto es una figura de incorporación reciente y desaparece en el derecho procesal argentino.

En este punto es importante establecer una diferencia entre la interceptación "tradicional" de comunicaciones, generalmente receptada en las legislaciones analizadas, y la interceptación de comunicaciones cifradas. Mientras que la primera refiere a la comunicación en sí misma, con el advenimiento del cifrado de las comunicaciones y los canales encriptados lo que se interviene son los dispositivos de quien emite y quien recibe. Esta última forma implica una injerencia mucho mayor que la tradicional y, como veremos, no está aún óptimamente receptada en los Códigos Procesales. Esto puede representar un riesgo aún mayor si, frente a la falta de regulación específica, se aplican por analogía las reglas de la intervención tradicional, por su naturaleza menos invasiva que esta técnica y por ende con menos salvaguardas. Es por eso que en esta investigación la consideramos como una herramienta de

investigación igual de intrusiva que el allanamiento remoto y que también requerirá necesariamente para su ejecución el uso de softwares tipo *spyware*.

En este escenario, exploramos regulaciones de países que consideramos que establecen un marco habilitante que respeta mínimamente derechos y garantías (España y Reino Unido, principalmente), como los principios que surgen del Convenio de Budapest sobre Ciberdelincuencia (Ley Nacional N.º 27.411). Entre los estándares mínimos encontramos la exigencia de autorización judicial previa mediante resolución fundada, excepcionalidad y subsidiariedad de la medida, delimitación precisa de los delitos que la habilitan, plazos máximos de duración con posibilidad de prórroga justificada, protección de datos sensibles y de las comunicaciones amparadas por secreto profesional, y garantías de cadena de custodia e intangibilidad de la información obtenida<sup>1</sup>.

Sobre esta base analizamos la regulación a nivel federal (Código Procesal Penal Federal) y de las 24 jurisdicciones que integran el país (códigos procesales penales locales). **Nos abocamos principalmente al análisis comparativo de dos técnicas de investigación: la interceptación de comunicaciones (aplicada también a comunicaciones cifradas) y el allanamiento remoto.**

## → EL ANÁLISIS NORMATIVO DE LAS 25 JURISDICCIONES. NIVELES DE RIESGO

En función del relevamiento de las regulaciones normativas y las respuestas recibidas, complementado con respuestas a las solicitudes de información cuando las hubo (especialmente para analizar el tipo de interpretación que las autoridades hacen sobre la norma), categorizamos a las distintas jurisdicciones (provincias, CABA y régimen federal) en 4 grupos, a las que asignamos un nivel de “riesgo” en este sentido:

---

<sup>1</sup> Para más detalles sobre las garantías recomendamos la lectura de CELS, O.D.I.A, Fundación Vía Libre y Democracia en Red, [“Alerta Spyware”](#), junio 2026, realizado con el apoyo de New Venture Fund.

**1. Riesgo alto:** aquellas que habilitan normativamente herramientas intrusivas de manera expresa, sin perjuicio de la falta de respuesta a los PDI, o cuyas autoridades confirmaron la interpretación amplia en el caso de poseer legislaciones ambiguas a través de su respuesta al pedido de información particular. En este nivel tenemos 10 jurisdicciones.

A su vez, en esta categoría se distinguen dos subcasos. Por un lado, nueve provincias cuyos códigos incorporan expresamente la figura del allanamiento remoto o el uso de programas informáticos: Chubut (art. 181 CPP y art. 14 Ley complementaria XV 43)<sup>2</sup> Corrientes (art. 217 CPP), La Pampa (art. 183 CPP), La Rioja (art. 165 CPP del nuevo código entrado en vigencia en junio 2025)<sup>3</sup>, Misiones (art. 283 ter CPP), Neuquén (art. 153 CPP), Salta (art. 309 sexies CPP), San Luis (art. 139 CPP) y Tucumán (art. 199 CPP).

Por otro lado, Córdoba: el artículo 216 de su CPP no incorpora expresamente estas herramientas, pero sí habilita la intervención "cualquiera sea el medio técnico utilizado", y la respuesta al PDI confirmó una interpretación institucional amplia, por lo que lo incluimos en la categoría de riesgo "rojo".

**2. Riesgo medio:** aquellas jurisdicciones que podrían habilitar herramientas normativas (no lo hacen de manera expresa pero tienen disposiciones laxas que podrían permitir utilizarlas). Este grupo lo estudiamos especialmente a través de los PDIs, para intentar conocer la interpretación que los operadores judiciales hacen del texto legal. En función de esto, las dividimos en dos subgrupos:

- 
- 2 El Código Procesal Penal de Chubut fue reformado a través de la Ley provincial XV 43 durante el período de relevamiento e investigación para este informe, por lo que no fue posible cursar un PDI a las autoridades sobre la nueva normativa. Para este análisis en principio nos basamos en el texto legal previo a la reforma, que gozaba de la posibilidad de habilitar *spyware* según interpretación. Con la sanción de la Ley XV 43, complementaria al CPP chubutense, se habilitó expresamente a través de sus arts. 14 y 15 la interceptación de los medios de comunicación o de las terminales y el allanamiento remoto, respectivamente.
  - 3 El Código Procesal Penal de La Rioja fue reformado durante el período de relevamiento e investigación para este informe, por lo que no fue posible cursar un PDI a las autoridades sobre la nueva normativa. Para este análisis nos basamos exclusivamente en el texto legal, que incorpora la habilitación expresa para procedimientos que implican el uso de software.

**2.a. Riesgo medio-alto:** Aquellas que podrían habilitar normativamente herramientas intrusivas y la respuesta recibida permite deducir una interpretación amplia, en tanto no se expresan en sentido contrario. Nos referimos a casos donde la respuesta se limita, por ejemplo, a afirmar que no se adquirieron a la fecha tecnologías de vigilancia pero que no niegan que exista la habilitación para hacerlo. Esta inferencia sobre la interpretación amplia se explica también en función del contexto en el que se da: en un escenario de creciente adquisición de tecnologías por parte de los distintos Estados —especialmente para vigilancia— y de reforma de Códigos Procesales en varias jurisdicciones en el sentido de incorporar su uso, el hecho de que las autoridades se limiten a contestar otras cuestiones (siempre de forma escueta) y no aborden ni nieguen expresamente la interpretación amplia de estas previsiones legales, levanta una fuerte alarma sobre su lectura de la habilitación.

Esta categoría incluye a 8 jurisdicciones: Buenos Aires (art. 229 CPP), CABA (art. 124 CPP), Entre Ríos (art. 283 CPP), Mendoza (art. 229 CPP), Santa Cruz (art. 220 CPP), Santa Fe (art. 171 CPP), el nivel federal (art. 150 CPPF) y Neuquén (arts. 150 y 151 CPP).

En el caso de Neuquén, cabe aclarar que figura en ambas categorías: cuenta con habilitación expresa de allanamiento remoto (art. 153) y, adicionalmente, el PDI confirmó una interpretación amplia de sus normas de interceptación, aunque señaló que aún no se ha contratado software.

**2.b. Riesgo medio-bajo:** aquellas jurisdicciones que podrían habilitar el uso de herramientas intrusivas pero no respondieron el PDI, por lo que desconocemos la interpretación institucional y no parece haber obstáculos en los códigos procesales si se decidiera avanzar en el ejercicio de estas facultades.

Esta categoría incluye 7 jurisdicciones: Catamarca (art. 225 CPP), Formosa, Jujuy (art. 231 CPP), Río Negro (arts. 145-146 CPP), San Juan (arts. 243 y 244), Santiago del Estero (art. 253 CPP) y Tierra del Fuego (art. 211 CPP).

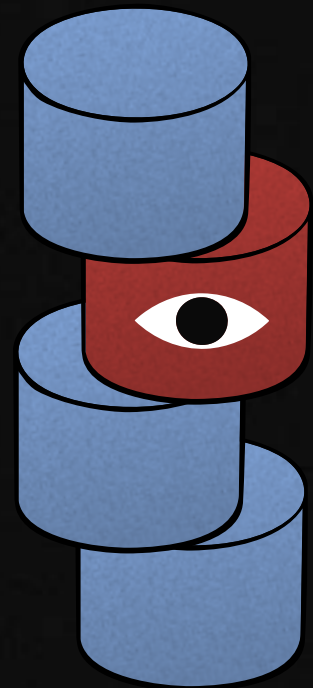
**3. Riesgo bajo:** finalmente, establecimos esta categoría para aquellas jurisdicciones que no habilitan normativamente herramientas intrusivas. De su código procesal no se desprende ninguna habilitación clara para utilizar *spyware*, por ejemplo para allanamiento remoto o intervención de comunicaciones. Verificamos este escenario en un solo caso, la provincia de Chaco (arts. 213 y 214 CPP) que, a su vez, ratificó esta lectura a través de su respuesta al PDI.

El detalle de cada jurisdicción -normas aplicables del CPP y respuesta obtenida, si la hubo- puede consultarse en el Anexo.

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 NIVEL DE IMPLEMENTACIÓN REAL: RESULTADOS DE LOS PEDIDOS DE INFORMACIÓN

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 NIVEL DE IMPLEMENTACIÓN REAL: RESULTADOS DE LOS PEDIDOS DE INFORMACIÓN

### → SÍNTESIS SOBRE LAS RESPUESTAS RECIBIDAS

De las 25 jurisdicciones relevadas, 12 respondieron los pedidos de información. En ninguno de estos casos se reportó la existencia de protocolos específicos de uso de *spyware* ni guías de buenas prácticas.

Algunos hallazgos para destacar: Chaco confirmó que no existe interpretación amplia de sus normas; fue la única jurisdicción en hacerlo. San Luis y Neuquén confirmaron que la facultad legal existe pero que aún no se ha adquirido software. Córdoba reportó una interpretación institucional amplia. Otro conjunto de jurisdicciones no rechazaron esta lectura, aún siendo específicamente preguntados al respecto (Buenos Aires, Chubut, CABA, Entre Ríos, Mendoza, Santa Cruz, Santa Fe y el nivel federal).

Además, salvo dos excepciones (San Luis y Neuquén) las jurisdicciones que tienen regulada normativamente la posibilidad de utilizar herramientas intrusivas en general no respondieron el PDI, a pesar de la grave amenaza para los derechos que implica la habilitación que tienen. Y, quienes no tienen regulada esta posibilidad pero tienen disposiciones que podrían habilitarla, en general contestaron únicamente informando no haber contratado tecnologías, sin profundizar sobre cómo interpretan las normas.

Por otro lado, del universo de respuestas recibidas, la mayoría parece no entender de qué se trata el uso de herramientas intrusivas de este tipo. Confunden, por ejemplo, allanamiento remoto con extracción física de datos de dispositivos móviles. Esto es particularmente preocupante en un contexto de progresiva habilitación de estas herramientas y reformas de los Códigos en este sentido, a lo largo del país.

## → LA FALTA DE RESPUESTA COMO PROBLEMA POLÍTICO

13 jurisdicciones no respondieron los pedidos de información. Este dato no puede tratarse como una deficiencia administrativa menor. En un campo donde las herramientas disponibles representan una alta intrusión en la vida de las y los ciudadanos, en tanto permiten vigilar de forma encubierta a cualquier persona sin que ésta lo sepa, la opacidad institucional tiene consecuencias directas sobre el ejercicio de derechos fundamentales.

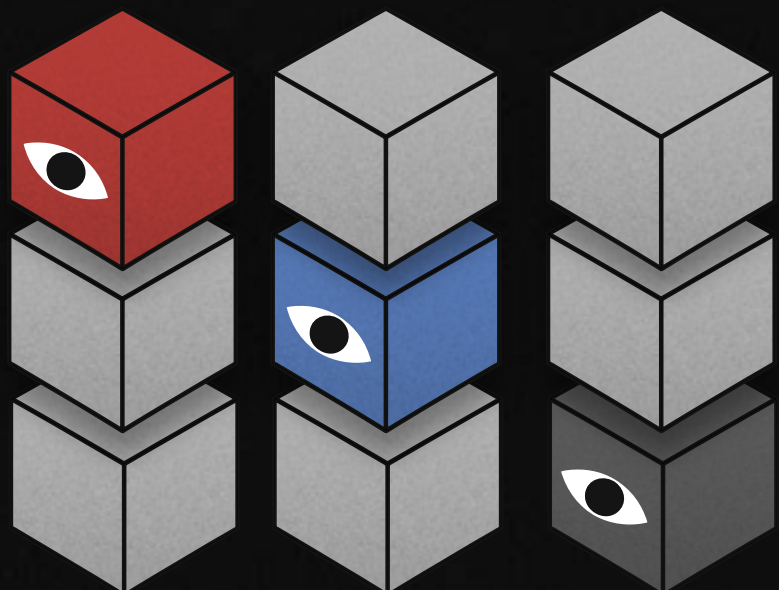
La falta de respuesta impide saber si las autoridades se consideran, en gran parte de los casos, habilitadas a ejercer este tipo de facultades. Tampoco nos permite conocer si se adquirieron herramientas de vigilancia y en ese caso, quién tomó la decisión, con qué presupuesto y bajo qué salvaguardas y controles. Esto es especialmente grave en las provincias con habilitación legal expresa que no respondieron: como es el caso de Corrientes, La Pampa, Misiones, Salta y Tucumán, que cuentan con normas que habilitan el allanamiento remoto o el uso de *spyware*, pero no informaron nada sobre su implementación práctica.

La falta de información representa una dificultad para el control público, que a su vez redundó en un aumento significativo del riesgo de usos abusivos e ilegales. En este sentido, los estándares internacionales en la materia son claros en que cuanto más invasiva es la facultad estatal, mayor es el deber de rendición de cuentas y mecanismos de control. Sin embargo, las capacidades de control de los diferentes poderes del Estado y de la sociedad civil sobre los asuntos vinculados a la seguridad, la investigación criminal, la inteligencia y la defensa siempre fueron débiles en la Argentina. En los últimos años esta característica se fue acentuando: es cada vez más difícil que policías, espías, funcionarios y judiciales rindan cuentas de lo que hacen, y la experiencia con estas solicitudes de información confirma la tendencia.

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 Y HALLAZGOS TRANSVERSALES

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 Y HALLAZGOS TRANSVERSALES

### → FRAGMENTACIÓN NORMATIVA Y ASIMETRÍA ENTRE PROVINCIAS

Por su característica federal, Argentina no tiene un marco normativo uniforme a nivel nacional sobre la habilitación para el uso de tecnologías intrusivas en investigaciones penales. El resultado es un mapa de veinticinco regímenes dispares: provincias como Salta han incorporado expresamente el uso de software espía sin conocimiento del imputado, mientras otras ni siquiera regulan el allanamiento remoto. Estas diferencias implican protecciones disímiles, sin un estándar mínimo de salvaguardas y/o mecanismos de control exigidos. A la vez, permiten lagunas o zonas de opacidad que pueden ser aprovechadas sin control.

### → BRECHAS GENERALIZADAS EN LAS GARANTÍAS Y FALTA DE PROTOCOLOS ESPECÍFICOS

De lo anterior se desprenden brechas incluso entre las jurisdicciones con mayor desarrollo normativo: ausencia de criterios de proporcionalidad, falta de restricción a delitos habilitantes, protección insuficiente de datos sensibles, plazos excesivos o indefinidos, y ausencia de mecanismos de notificación posterior al imputado. De hecho, casi ninguna jurisdicción cuenta con protocolos de uso, guías de buenas prácticas o mecanismos de registro y reporte. La brecha entre la existencia de la facultad legal y la existencia de reglas para su ejercicio es uno de los déficits más preocupantes.

## → AUMENTO PROGRESIVO DE LA INCORPORACIÓN DE ESTAS TÉCNICAS

Desde una perspectiva temporal, la incorporación normativa del allanamiento remoto u otras figuras que implican la utilización de *spyware* se produjo en los últimos años: es el caso de Neuquén (2014), La Pampa y Corrientes (2020), San Luis (2021), Salta (2023), Misiones (2024) y, más recientemente, La Rioja (2025). Esta progresión muestra una tendencia sostenida de ampliación de estas facultades, frecuentemente por delante de cualquier debate público o parlamentario sobre sus implicancias para los derechos fundamentales.

## → FALTA DE CAPACITACIONES PARA UN USO RESPETUOSO DE LOS DDHH

De las respuestas recibidas se desprende poca claridad de los operadores sobre qué significa *spyware* y cuál es su diferencia con otros softwares u otras técnicas de investigación. En la medida en que aumenta la incorporación de estas herramientas en los Códigos, es indispensable crear conocimiento técnico para su utilización responsable.

## → LA HABILITACIÓN IMPLÍCITA COMO PRINCIPAL FACTOR DE RIESGO.

La categoría de mayor riesgo no es necesariamente la de las provincias con habilitación expresa, sino la de aquellas que habilitan el uso de *spyware* por vía de interpretación amplia de normas genéricas de interceptación, sin que esa interpretación esté formalizada ni sujeta a controles específicos y protocolos de uso. Por ejemplo, los plazos máximos regulados para interceptaciones tradicionales dejarían de ser proporcionales cuando se trata de interceptación de comunicaciones cifradas, en tanto se trata de una medida coercitiva mucho mayor: implica acceder al dispositivo completo. Tampoco hay garantías explícitas: no hay plazos diferenciados, restricción de delitos habilitantes ni protección reforzada de datos sensibles, entre otras.

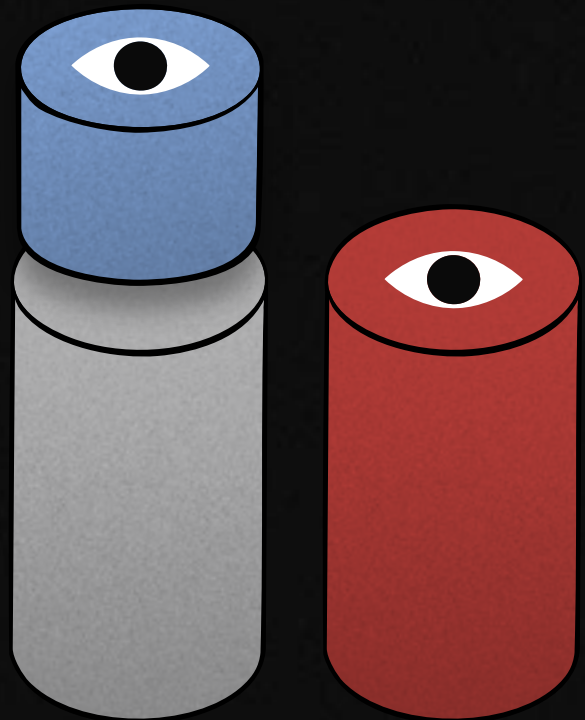
## → EL SILENCIO INSTITUCIONAL

La falta de respuesta a los pedidos de información de más de la mitad de las jurisdicciones no es un problema únicamente administrativo, sino que se convierte en un problema político. En una materia tradicionalmente opaca, como es la vigilancia estatal, una vez más nos encontramos con restricciones a la rendición de cuentas, a la transparencia y a la auditabilidad de los sistemas utilizados. En este caso, además, redunda también en un problema para el ejercicio del derecho a la defensa.

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

# ANEXO

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



## ANEXO

### → ANÁLISIS NORMATIVO POR JURISDICCIÓN

A continuación se presenta el análisis de cada jurisdicción, organizado conforme a las cuatro categorías antes desarrolladas. Para cada una se indica la norma aplicable, el tipo de habilitación, las garantías previstas y sus lagunas, y el resultado del pedido de información.

#### 1. JURISDICCIONES CON HABILITACIÓN EXPRESA DE ALLANAMIENTO REMOTO O USO DE SPYWARE, O CON INTERPRETACIÓN AMPLIA CONFIRMADA POR PDI

##### » CHUBUT

La respuesta al PDI confirmó una posible interpretación amplia. De hecho, al momento del relevamiento se debatía un proyecto de ley que incorporaría habilitación expresa para vigilancia digital.

Como mencionamos en el documento principal, durante el período del relevamiento para este trabajo Chubut sancionó una nueva ley complementaria que regula específicamente (Ley provincial XV 43) el uso de herramientas tecnológicas en la investigación, prevención y lucha contra los delitos complejos y de cibercriminalidad, más precisamente a través de sus artículos 14 y 15.

En consecuencia, a diferencia de las demás provincias de esta categoría, no realizamos un pedido de información actualizado con respecto a la normativa actual, en tanto su entrada en vigencia sucedió luego del período de investigación. Por tanto, el análisis se basa exclusivamente en la nueva normativa que habilita herramientas intrusivas de forma expresa.

## » CORRIENTES

El artículo 217 del CPP autoriza expresamente el acceso remoto al contenido de dispositivos y sistemas informáticos mediante software. El artículo 216 exige autorización judicial y establece que la medida sólo es aplicable en la investigación de delitos de especial gravedad (art. 213), a la vez que exige que sea registrada mediante medio técnico idóneo para asegurar su validez probatoria y la protección de los datos personales.

Además, prevé que el juez debe realizar un control de razonabilidad que descarte la existencia de otras medidas de investigación menos gravosas para el derecho a la intimidad del investigado que resulten igualmente útiles para el fin pretendido (entre otras, art. 210). En este sentido, el artículo 13 del Código establece expresamente el deber de respetar el derecho a la intimidad, incluyendo datos personales en formato digital y comunicaciones electrónicas.

También habilita expresamente el allanamiento remoto: el art. 217 indica que podrá autorizarse con respecto al contenido de ordenadores, dispositivos electrónicos, sistemas informáticos, bases de datos o instrumentos de almacenamiento masivo de datos informáticos, a través de un software que lo permita o facilite; y que el juez podrá exigir al fiscal que precise la forma en que se procederá al acceso y captación de los datos o archivos informáticos, así como la identificación del software mediante el cual se ejecutará el control de la información.

Esta provincia no respondió el PDI.

## » LA PAMPA

El artículo 182 habilita la intervención de comunicaciones “telefónicas o por cualquier otro medio”, alcanzando también a terceras personas vinculadas al proceso. La norma exige orden judicial, pero no establece garantías específicas adicionales para la modalidad remota ni criterios de proporcionalidad.

Por su parte, el artículo 183 del CPP sobre evidencia digital prevé, entre otras facultades, el registro o intervención del dispositivo por medios técnicos y/o en forma remota, con autorización judicial y sin afectar las comunicaciones con defensores. Prevé que los datos extraídos se conserven sólo por “un plazo razonable”, sin mayores precisiones.

No respondió el PDI.

## » LA RIOJA

El artículo 165 del nuevo CPP provincial incorpora habilitación expresa para la interceptación de comunicaciones en general, lo que incluye la posibilidad de uso de *spyware*.

Como mencionamos en el documento principal, durante el período del relevamiento para este trabajo La Rioja reformó su Código. En consecuencia, a diferencia de las demás provincias de esta categoría, no realizamos un pedido de información actualizado con respecto a la normativa actual, en tanto su entrada en vigencia sucedió luego del período de investigación. En consecuencia, el análisis se basa exclusivamente en la nueva norma.

## » MISIONES

El artículo 237 habilita la interceptación de comunicaciones telefónicas o de cualquier otro medio de comunicación, lo que hace que sea factible extender la interceptación a comunicaciones de tipo electrónico, sean cifradas o no. A la vez, el artículo 283 ter habilita al juez a ordenar, mediante auto fundado, la obtención de evidencias y datos de manera remota a través del uso de programas y herramientas informáticas forenses y otros mecanismos tecnológicos. Así, la conjunción de ambas normas habilita al Estado a contratar y usar herramientas de software.

No respondió el PDI.

## » NEUQUÉN

El artículo 153 del CPP habilita el registro del dispositivo por medios técnicos y en forma remota cuando las circunstancias del caso hacen presumir que contiene información útil para la investigación. Los artículos 150 y 151 regulan la interceptación de comunicaciones con exigencia de resolución fundada del Juez de Garantías a pedido de parte, plazos máximos (diez días para interceptación telefónica, hasta noventa días totales con renovaciones justificadas) y protección de las comunicaciones con defensores.

Neuquén es una de las únicas dos provincias de esta categoría que respondieron el PDI: confirmó la interpretación amplia de sus normas de interceptación, pero señaló que aún no ha contratado software de este tipo.

## » SALTA

El artículo 309 sexies del CPP regula la obtención de datos de forma remota y sin el conocimiento del titular o usuario del dispositivo, mediante la utilización de programas informáticos (*spyware*) u otros mecanismos tecnológicos.

El artículo 316 habilita la interceptación de comunicaciones telefónicas y online cursadas por cualquier medio, con garantías y a través de determinados mecanismos tecnológicos (remite al art. 309 sexies para esta cuestión). No se prevé una lista taxativa de delitos habilitantes.

No respondió el PDI.

## » SAN LUIS

El artículo 139 del CPP habilita el registro remoto con autorización judicial que incluya fundamentación y alcance específico (aunque no menciona expresamente la proporcionalidad como requisito), y establece un plazo máximo de conservación de noventa días. Para la interceptación de comunicaciones prohíbe expresamente las comunicaciones con defensores y establece plazos breves. No aborda la protección de datos sensibles ni

delimita delitos habilitantes. Es la única provincia de esta categoría, además de Neuquén, que respondió el PDI: confirmó que la facultad legal existe pero que aún no se ha adquirido software.

## » TUCUMÁN

El artículo 196 del CPP autoriza la interceptación “por cualquier medio técnico”, incluyendo la obtención en tiempo real de datos de tráfico y contenido. A la vez, el artículo 199 habilita expresamente el registro del dispositivo por medios técnicos y en forma remota. Estas medidas tienen carácter excepcional, exigen autorización judicial y no pueden superar los noventa días prorrogables con justificación.

No respondió el PDI.

## » CÓRDOBA

El artículo 216 del CPP permite la intervención de comunicaciones “cualquiera sea el medio técnico utilizado, para impedir las o conocerlas”, mediante auto fundado. No establece plazos, criterios de proporcionalidad, protección de datos sensibles ni lista de delitos habilitantes. Aunque no prevé expresamente el allanamiento remoto -pero tampoco lo prohíbe-, el PDI confirmó una interpretación institucional amplia que equipara en la práctica a Córdoba con las provincias de habilitación expresa.

## 2. JURISDICCIONES CON HABILITACIÓN POSIBLE POR INTERPRETACIÓN AMPLIA Y PDI RESPONDIDO QUE LO CONFIRMA

### » BUENOS AIRES

El artículo 229 del CPP habilita la interceptación de comunicaciones con autorización judicial 'cuando existan motivos que lo justifiquen y mediante auto fundado'. El artículo no refiere a plazos, resguardo de información ni protección de datos sensibles. No prevé allanamiento remoto de manera expresa.

La respuesta al PDI permite inferir una interpretación amplia (en tanto no se aclara lo contrario) que habilitaría herramientas intrusivas.

### » CIUDAD AUTÓNOMA DE BUENOS AIRES

El CPP de la CABA regula las interceptaciones en los artículos 123 y 124, de carácter excepcional, con autorización judicial fundamentada, confidencialidad y bajo la prohibición respecto a las comunicaciones con la defensa.

No se prevé el allanamiento remoto.

La respuesta al PDI parece confirmar que podría existir una interpretación amplia -no la niega-, aunque no accedimos a una interpretación institucional unificada ni documentos generales que la establezcan.

### » ENTRE RÍOS

Los artículos 281 y 283 del CPP prevén la interceptación de correspondencia y de comunicaciones telefónicas y por cualquier otro medio, incluyendo en línea.

Exigen autorización judicial por auto fundado, justificando la proporcionalidad de la medida, en condiciones de confidencialidad y resguardando toda aquella información que no resulte necesaria a los fines de la investigación. Excluyen las comunicaciones con defensores.

No se prevé el allanamiento remoto.

La respuesta al PDI confirmó una posible interpretación amplia.

## » MENDOZA

El artículo 229 del CPP habilita la intervención de comunicaciones del imputado "cualquiera sea el medio técnico utilizado", y establece un plazo máximo. Esto implica que, si el imputado utilizara un método cifrado de mensajería instantánea, podría habilitarse su intervención mediante un *spyware* para poder conocer el contenido de las comunicaciones. La respuesta al PDI no contradice esta interpretación.

## » SANTA CRUZ

El artículo 220 del CPP autoriza la interceptación con orden judicial fundada, pero no contempla específicamente el allanamiento remoto. No establece estándares sobre proporcionalidad, protección de datos sensibles, ni plazos máximos.

La respuesta al PDI confirmó una posible interpretación amplia.

## » SANTA FE

Los artículos 171 y 172 del CPP permiten la interceptación con decreto fundado y protegen las comunicaciones con abogados, pero no establecen plazos máximos ni prevén una serie de delitos habilitantes.

No se contempla específicamente el allanamiento remoto.

El PDI confirmó una posible interpretación amplia.

## » NIVEL FEDERAL

El Código Procesal Penal Federal (CPPF) -modificado en 2019 por Ley 27.482, de paulatina implementación y por lo tanto con vigencia efectiva limitada- regula la interceptación de comunicaciones en el artículo 150, de cualquier tipo, de modo análogo al allanamiento. Es una cláusula abierta que, como vimos en otros casos, puede entenderse como una habilitación para el uso de *spyware* cuando las comunicaciones estén cifradas o no puedan interceptarse por medios convencionales.

Se prevé plazo máximo, deber de confidencialidad y obligación de colaboración de terceros (empresas de comunicaciones), así como la exigencia de evaluar la legalidad y la razonabilidad de la medida, y mantener la medida sólo mientras estas circunstancias se mantengan.

No se contempla expresamente el allanamiento remoto.

En la respuesta al PDI, las autoridades explicaron que no hay contratada tecnología espía pero no se opusieron a la interpretación normativa que los habilitaría a tenerla y utilizarla.

### 3. JURISDICCIONES CON HABILITACIÓN POSIBLE POR INTERPRETACIÓN AMPLIA Y SIN RESPUESTA AL PDI

## » CATAMARCA

El artículo 225 del CPP habilita la intervención de comunicaciones del imputado "cualquiera sea el medio técnico utilizado, para impedir las o conocerlas", mediante decreto fundado. Esta fórmula amplia podría interpretarse como habilitación implícita para el uso de *spyware*.

No se contempla expresamente el allanamiento remoto.

No respondió el PDI.

## » FORMOSA

El CPP de Formosa permite, a través de su art. 213, la interceptación de comunicaciones con orden judicial, sin establecer estándares de proporcionalidad, protección de datos sensibles ni plazos específicos, así como tampoco prevé una lista de delitos habilitantes.

No se contempla expresamente el allanamiento remoto.

No respondió el PDI.

## » JUJUY

El artículo 231 del CPP habilita la interceptación de correspondencia postal, telegráfica, electrónica "o cualquier otra forma de comunicación o de todo otro efecto", con carácter excepcional y plazo máximo. El juez debe controlar la legalidad y razonabilidad del requerimiento. La norma remite expresamente al Convenio de Budapest (Ley N° 27.411), lo que podría reforzar una interpretación que habilite el uso de *spyware*.

No se contempla expresamente el allanamiento remoto.

No respondió el PDI.

## » RÍO NEGRO

Los artículos 145 y 146 del CPP regulan la intervención de comunicaciones en general y telefónicas en particular, con orden judicial, plazo máximo y bajo condiciones de necesidad. A su vez, el artículo 148 prevé la "incautación de datos" de equipos informáticos secuestrados, medida distinta al allanamiento remoto.

No respondió el PDI.

## » SAN JUAN

El CPP de San Juan regula la interceptación e intervención de comunicaciones, y la incautación de datos (arts. 243, 244 y 245 respectivamente). Permite la interceptación de comunicaciones con orden judicial justificada, establece un plazo máximo, obliga a terceros (empresas telefónicas) a colaborar, protege la confidencialidad de la información obtenida y dispone la destrucción de aquella irrelevante. No prevé una lista de delitos habilitantes. A la vez, regula el allanamiento remoto con incautación de datos, modalidad que en la práctica puede requerir el uso de *spyware* para acceder a dispositivos bloqueados o cifrados. No distingue datos sensibles ni protege el secreto profesional.

No respondió el PDI, por lo que no conocemos su interpretación.

## » SANTIAGO DEL ESTERO

El artículo 253 del CPP prevé la interceptación y el secuestro de correspondencia de distinto tipo, entre ellos cibernética, mediante auto fundado del juez, justificando su utilidad para la comprobación del delito y previendo la devolución de lo secuestrado cuando no se encontrara nada relevante. No es claro si esto último se aplica también al cese de la interceptación.

Así las cosas, se podrían habilitar herramientas intrusivas por interpretación. No regula el allanamiento remoto.

No respondió el PDI.

## » TIERRA DEL FUEGO

El CPP de Tierra del Fuego, Antártida e Islas del Atlántico Sur exige orden judicial fundada para interceptar comunicaciones (art. 211), sin mayores detalles sobre el alcance, plazos o protecciones específicas.

Tampoco contempla específicamente el allanamiento remoto, por lo que no establece estándares sobre autorización judicial, proporcionalidad, protección de datos sensibles, ni otros aspectos relevantes.

No respondió el PDI.

#### 4. JURISDICCIONES QUE NO HABILITAN NORMATIVAMENTE HERRAMIENTAS INTRUSIVAS

##### » **CHACO**

El art. 215 autoriza la interceptación de comunicaciones telefónicas en el marco de procesos penales, lo que podría dar lugar a interceptación de comunicaciones cifradas, que requeriría el uso de *spyware*.

Sobre este punto, las autoridades del Ministerio Público Fiscal provincial informaron que “en relación con las comunicaciones digitales transmitidas mediante mensajerías cifradas, correos electrónicos o redes sociales, debe señalarse que hasta el presente no se ha considerado en esta jurisdicción la aplicación extensiva del art. 215 para habilitar dichas medidas”, lo cual coloca a Chaco en la categoría “verde” de nuestro análisis.

