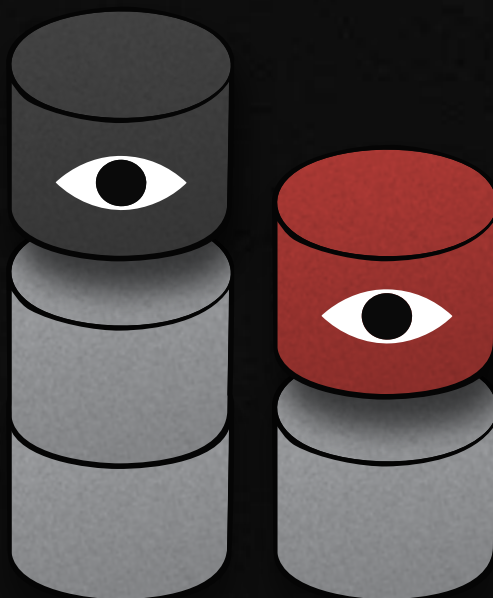


0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0
0 1 0 1 0 1
1 0 1 0 1 0

/TECNOLOGÍAS INTRUSIVAS:

**ESTÁNDARES DEL DERECHO INTERNACIONAL
DE LOS DERECHOS HUMANOS APLICABLES
A SU USO POR PARTE DE LOS ESTADOS**

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



"Tecnologías intrusivas: estándares del derecho internacional de los derechos humanos aplicables a su uso por parte de los Estados"

Autoría: Margarita Trovato
Dirección del proyecto: Beatriz Busaniche

Realizado con el apoyo de **Spyware Accountability Initiative** en el marco del proyecto "El camino del espionaje en Argentina: proteger el espacio cívico y reforzar la capacidad de la sociedad civil", integrado por el **Centro de Estudios Legales y Sociales (CELS)**, **Democracia en Red**, la **Fundación Vía Libre** y el **Observatorio Argentino de Derecho Informático (O.D.I.A.)**.

Buenos Aires, agosto de 2026

Este documento se distribuye bajo los términos de la licencia
Creative Commons Atribución – Compartir Obras Derivadas Igual
Internacional

<https://creativecommons.org/licenses/by-sa/4.0/>

© Centro de Estudios Legales y Sociales, Democracia en Red,
Fundación Vía Libre y Observatorio Argentino de Derecho
Informático (2026).

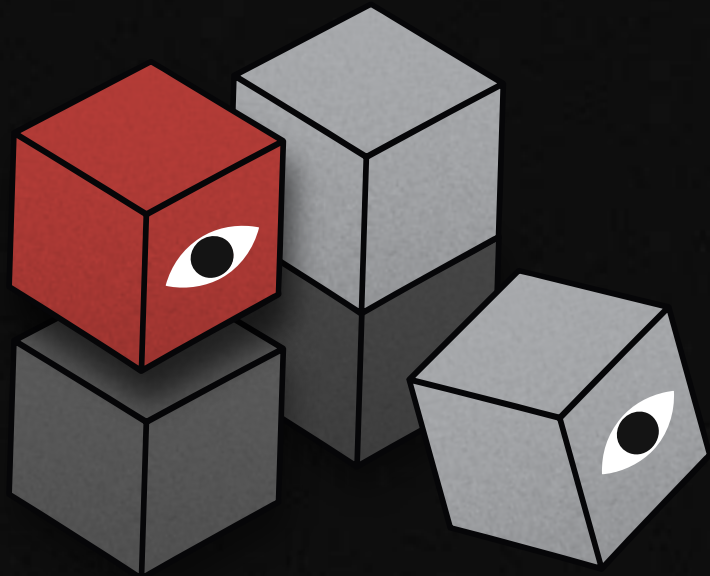
ÍNDICE

4	Introducción
8	Estándares
9	I. Previo a la utilización de la tecnología
16	II. Durante la ejecución de la medida
20	III. Una vez finalizada la medida
24	Conclusión

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 documento **compila estándares internacionales sobre el uso de tecnologías de vigilancia intrusivas por parte de los Estados, entre las que se incluyen las de software espía o *spyware***, entendidas como aquellos programas que permiten infiltrarse de manera encubierta en una computadora personal, un teléfono móvil u otro dispositivo digital para activar cámara o micrófono, rastrear la actividad del dispositivo, y acceder, modificar o borrar la información allí almacenada. En otras palabras, ejercer un control absoluto sobre el dispositivo infiltrado ¹.

El *spyware* no es una forma más de vigilancia tradicional, sino una tecnología cualitativamente distinta por lo que permite hacer con el dispositivo intervenido. Es por esa razón que, si bien los estándares internacionales desarrollados para la vigilancia de comunicaciones y las actividades de inteligencia estatal en general resultan aplicables a su uso, también hay un consenso sobre los deberes reforzados de los Estados respecto a la garantía de derechos al utilizarlo. En este sentido, la mayoría de los estándares reunidos en este documento se desarrollaron para interceptación telefónica, allanamientos o recolección de datos personales en general mediados por tecnologías, y resultan aplicables por extensión analógica. En los casos en que las fuentes sí hacen referencia expresa a *spyware*, lo indicamos.

En este documento trabajamos sobre fuentes del derecho internacional de los derechos humanos de distinto peso jurídico y político para la Argentina. Por un lado, abordamos normativa vinculante: el Convenio 108 del Consejo de Europa² y su protocolo de actualización, Convenio 108+ ³. También relevamos decisiones de organismos internacionales de los que la Argentina

1 Corte Interamericana de Derechos Humanos (Corte IDH), Caso Miembros de la Corporación Colectiva de Abogados "José Alvear Restrepo" (CAJAR) c. Colombia, Excepciones Preliminares, Fondo, Reparaciones y Costas, Sentencia de 18 de octubre de 2023, Serie C No. 506, nota al pie 688, *con cita a Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, A/69/397, 23 de septiembre de 2014.*

2 Consejo de Europa, *Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal* ("Convenio 108"), 1981. Se trata del Primer tratado internacional vinculante en materia de protección de datos personales; fija los principios generales de licitud del tratamiento y las condiciones para las excepciones por motivos de seguridad del Estado, entre otros fines. Argentina es parte, por lo que sus disposiciones le son vinculantes.

es parte (Sistema Interamericano y el Sistema Universal de Derechos humanos), entre ellas jurisprudencia, recomendaciones o informes de órganos de tratados y relatorías especiales. Por último, también hacemos referencia a decisiones de organismos de sistemas de los que la Argentina no es parte, como por ejemplo sentencias del Tribunal de Justicia de la Unión Europea (TJUE) o del Tribunal Europeo de Derechos Humanos (TEDH) que se incorporan como referencia de derecho comparado y entendiendo la relevancia del *soft law* para el impulso de buenas prácticas de los Estados.

Por razones metodológicas, presentamos los estándares relevados según el momento del despliegue de la tecnología al que se refieren: i) previo a su utilización, ii) durante la ejecución de la medida, y iii) una vez finalizada. Incluimos ejemplos concretos sobre afectaciones a derechos, que permiten destacar la relevancia de estos estándares al momento de la implementación de tecnologías de este tipo por parte de los Estados.

Por último, nos interesa distinguir dos supuestos de uso que atraviesan buena parte de los estándares reunidos. El primero es el uso en el marco de una investigación criminal de un posible delito, terreno en el que rigen las garantías del debido proceso, así como criterios de independencia y objetividad exigibles a los órganos que investigan. El segundo es el uso con fines de inteligencia, de naturaleza esencialmente preventiva y orientada a apoyar la toma de decisiones en materia de seguridad, no a la represión directa del delito. Aunque ambos supuestos pueden valerse de métodos similares (entre ellos, la vigilancia de comunicaciones o el uso de *spyware*, en este caso), sus finalidades difieren, y esto puede derivar en exigencias distintas en materia de autorización, control y acceso a la información obtenida. A lo largo del documento dejamos asentados estas particularidades cuando corresponde.

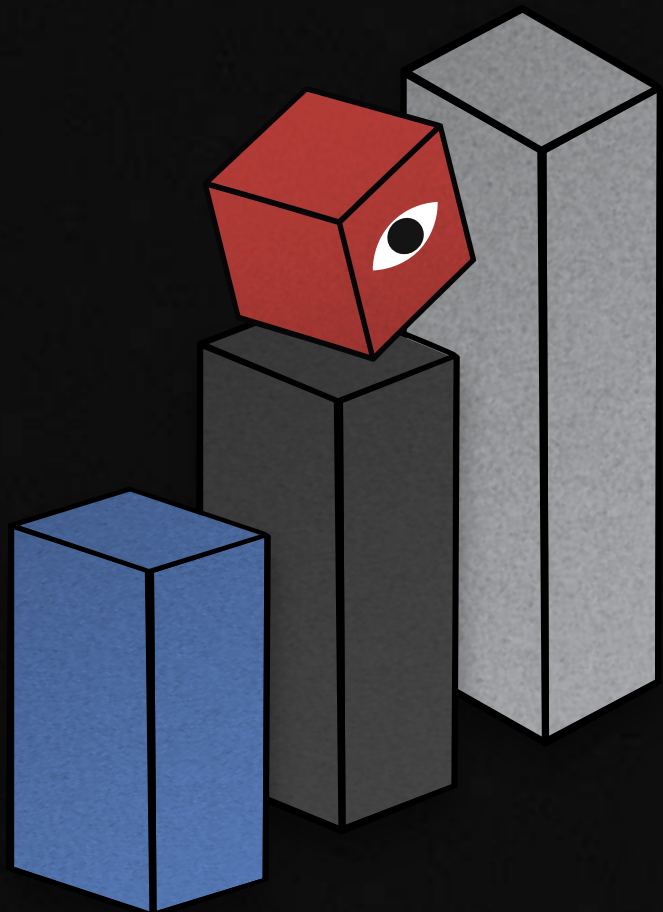
3 Consejo de Europa, *Protocolo de Enmienda al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal* ("Convenio 108+"), 2018. Moderniza el Convenio de 1981, incorporando, entre otras cosas, exigencias más estrictas para las excepciones por seguridad nacional y defensa (entre ellas, la revisión y supervisión independiente). A la fecha de elaboración de este documento, el Convenio 108+ aún no entró en vigor: requiere la ratificación de 38 Estados para hacerlo, y por el momento cuenta con 34.

Este relevamiento no pretende ser exhaustivo, pero sí reunir, con el mayor sustento normativo posible, los estándares más sólidos y convergentes entre los distintos sistemas de protección de derechos humanos. Su objetivo es servir de base técnica para evaluar la legalidad y legitimidad de marcos normativos, prácticas y propuestas regulatorias vinculadas al uso de tecnologías de vigilancia intrusivas, incluido el *spyware*, por parte del Estado.

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

ESTÁNDARES

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



ESTÁNDARES

I. PREVIO A LA UTILIZACIÓN DE LA TECNOLOGÍA

1. Legalidad, legitimidad, necesidad y proporcionalidad

Conocido como “test tripartito”, estas tres son condiciones que se exigen frente a cualquier restricción de derechos. Al tratarse de prácticas invasivas y potencialmente tan gravosas, según el derecho internacional se torna aún más estricto. En concreto, la Corte Interamericana de Derechos Humanos (Corte IDH) exige que la medida sea “absolutamente indispensable para conseguir el fin deseado”⁴, lo que el Alto Comisionado para los Derechos Humanos de las Naciones Unidas (OHCHR) agrega “la opción menos intrusiva disponible”⁵. En el mismo sentido, la Relatoría para la Libertad de Expresión (RELE) de la Comisión Interamericana de Derechos Humanos (CIDH) enfatiza en que la vulneración del derecho en cuestión no debe ser desmedida frente al beneficio que se obtiene con la medida⁶. La jurisprudencia europea, por su parte, pone el acento en la ley que lo habilita antes que en el uso en sí: exige que esta indique el alcance de la discrecionalidad estatal “con claridad suficiente” para evitar la arbitrariedad⁷. Aplicado específicamente a *spyware*, este test se traduce en una exigencia de último recurso o *última ratio*: el Alto Comisionado de Naciones Unidas sostiene que su uso sólo se justifica cuando las medidas menos intrusivas fueron agotadas o probadamente inútiles⁸. También hace referencia al universo que queda sujeto a estas técnicas: deberían utilizarse únicamente para la investigación “de una persona o de varias personas sospechosas de cometer o haber cometido tales actos”, no

4 Corte IDH, CAJAR, Op. Cit., párr. 537.

5 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR), *El derecho a la privacidad en la era digital. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, A/HRC/27/37, 30 de junio de 2014, párr. 22.

6 Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión (RELE), *El impacto de la vigilancia digital en la libertad de expresión en las Américas, 2025*, párr. 224.

7 Tribunal Europeo de Derechos Humanos (TEDH), *Gran Sala, Roman Zakharov vs. Rusia* (2015), párr. 230 y *Big Brother Watch y otros vs. Reino Unido* (2021), párrs. 347-350.

8 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR), *El derecho a la privacidad en la era digital. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, A/HRC/51/17, 4 de agosto de 2022, párr. 19.

de forma indeterminada ⁹.

1.1 El *spyware* podría ser incompatible con el requisito de necesidad y proporcionalidad, incluso cuando cumpla los demás elementos del test

Distintas fuentes advierten que, aun cuando una medida de *spyware* se verifique legal y legítima (requisitos que profundizaremos a continuación), la propia naturaleza de la tecnología dificulta que se cumplan las exigencias de necesidad y proporcionalidad. La Relatoría de Contraterrorismo de Naciones Unidas advierte que las capacidades inherentes del *spyware* pueden hacer imposible que su uso cumpla estos requisitos, precisamente porque no ofrece "capacidad operativa" para limitar qué datos recolecta¹⁰. El Alto Comisionado coincide: sostiene que herramientas como Pegasus u otras de *spyware* pueden afectar "la esencia misma" del derecho a la privacidad, no solo restringirlo, por su propio diseño¹¹. Corresponde a quien lo despliega probar que efectivamente se realiza en condiciones de necesidad y proporcionalidad, demostrando de qué manera se acota a estos requisitos.

1.2 La base legal de las actividades de inteligencia o vigilancia nunca puede ser secreta

Sobre la legalidad de la medida, la doctrina es clara en que el marco normativo que regula las actividades de este tipo debe definir con precisión sus fines y facultades, y su contenido "nunca puede ser de carácter reservado", de forma que las personas puedan conocer las

9 Ibidem

10 Relatoría Especial sobre la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo, *Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism*, A/HRC/52/39, 7 de febrero de 2023, párr. 44.

11 OHCHR, A/HRC/51/17, Op. Cit., párr. 19.

facultades del Estado y prever cómo podrían verse afectadas¹². En sentido similar el Alto Comisionado de Naciones Unidas para los DDHH agrega que la ley debe ser "públicamente accesible, precisa", y especificar con detalle las circunstancias de la interferencia, los procedimientos de autorización y los límites de duración, por lo que reglas o interpretaciones secretas no son admitidas¹³.

1.3 Las finalidades legítimas que habilitan la vigilancia deben ser taxativas, no pueden ser invocadas en abstracto y no deben ser discriminatorias

En cuanto a la legitimidad de la medida y teniendo en cuenta su potencial lesividad, es importante poner en juego el principio general de interpretación restrictiva de las excepciones. Aplicado al caso concreto, esto implica entender de manera limitada y taxativa aquello que habilitaría las actividades de vigilancia, en particular la legitimidad de la finalidad para la que se desplegaría la actividad.

Se entiende que sólo constituyen fines legítimos la seguridad nacional (entendida como protección de la existencia del Estado, su integridad territorial o su independencia política frente a amenazas concretas), el orden público, la salud pública y la protección de los derechos humanos¹⁴. Sin embargo, en tanto se trata de conceptos generales y amplios, los órganos del sistema interamericano tienen dicho que estos fines "no pueden invocarse en abstracto", sino que deben referirse a "amenazas específicas y concretas", y la seguridad nacional en particular no puede fundarse en una noción vaga sino en la protección de la existencia del Estado frente a amenazas definidas¹⁵. Este mismo principio lo retoma el Alto Comisionado de las Naciones Unidas, que exige que técnicas de *hacking*, como aquellas que habilita el *spyware*, se limiten a la prevención o investigación de "un delito grave específico o una amenaza grave y concreta a la seguridad nacional" ¹⁶.

12 Corte IDH, CAJAR, Op. Cit., párrs. 528-530.

13 OHCHR, A/HRC/27/37, Op. Cit., párrs. 28 y 29.

14 Corte IDH, CAJAR, Op. Cit., párrs. 531-533.

15 RELE (2025), Op. Cit., párr. 223.

16 OHCHR, A/HRC/51/17, Op. Cit., párr. 19.

Finalmente, los estándares son categóricos en cuanto a la prohibición de discriminación en los objetivos y/o posibles resultados de estas medidas: está vedado que las funciones de inteligencia y/o vigilancia estatal sean ejercidas para beneficiar o afectar a una persona o grupo en razón de su ideología, religión, opinión política o condición social¹⁷. La RELE puntualiza expresamente que no es un objetivo legítimo dirigirse a personas por su condición de disidentes políticos¹⁸. Si bien es una cuestión que muchas legislaciones internas receptan, la práctica parece ir en sentido contrario: la Relatoría de Protesta de ONU reveló recientemente que documentó un patrón de vigilancia por motivos de identidad y activismo en 84 Estados relevados¹⁹.

2. Autorización judicial previa obligatoria para toda medida invasiva

La Corte IDH explicó en CAJAR que aquellas "medidas invasivas de recopilación de información", como por ejemplo interceptación de comunicaciones y allanamiento de domicilios, deben ser siempre autorizadas de manera previa y expresa por autoridades judiciales independientes. Esta exigencia se extiende a cualquier técnica de vigilancia que implique "el acceso a bases de datos y sistemas de información no públicos que almacenen y procesen datos personales, el rastreo de usuarios en la red informática o la localización de dispositivos electrónicos" y, en el uso de *spyware*, también al acceso a "metadatos y datos telemáticos sensibles, como correo electrónico y metadatos de aplicaciones OTT, datos de ubicación, dirección IP, estación de torre celular, nubes de datos, GPS y Wi-Fi"²⁰. Esto es particularmente relevante en tanto estos programas permiten "ejercer el control absoluto del dispositivo infiltrado"²¹.

La RELE coincide: exige autorización judicial previa para toda medida invasiva de recopilación de información, con evaluación de idoneidad, necesidad y

17 Corte IDH, CAJAR, Op. Cit., párr. 535.

18 RELE (2025), Op. Cit., párr. 223.

19 Relatoría Especial sobre los derechos a la libertad de reunión pacífica y de asociación de las Naciones Unidas, *Los efectos disuasorios del ecosistema de vigilancia digital al descubierto: la erosión de los derechos de reunión y asociación*, A/HRC/62/45, 21 de abril de 2026, párrs. 5-9.

20 Corte IDH, CAJAR, Op. Cit., párrs. 542, 547, 551, 553 y nota al pie 688.

21 *Ibidem*, nota al pie 688, con cita Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, A/69/397, Op. Cit.

proporcionalidad por parte del juez en cada caso concreto²². Por su parte, la jurisprudencia europea sostiene, en la misma tónica, que la intervención "ofrece las mejores garantías de independencia, imparcialidad y procedimiento adecuado"²³, pero que esa autorización no puede basarse en una justificación genérica sobre la necesidad de controlar a una persona o categoría de personas: la decisión debe fundarse en "una sospecha individual respecto de la persona objetivo" para permitir una evaluación apropiada de necesidad y proporcionalidad en cada caso²⁴.

3. Evaluación de impacto en derechos humanos previa a cualquier despliegue de tecnología de vigilancia

La Relatora de protesta de ONU exige que todo despliegue de tecnología de vigilancia esté sujeto a evaluaciones de impacto en derechos humanos "integrales y no delegables" previas a su uso, que definan explícitamente propósito, alcance y población objetivo²⁵.

Que la evaluación deba ser "integral" implica no limitarse a medir el impacto sobre la privacidad de forma aislada, sino entender que los efectos de la vigilancia son "acumulados": afectan simultáneamente la privacidad, la libertad de expresión, la libertad de reunión, la libertad de asociación y la no discriminación, y la interdependencia entre esos derechos hace que "el daño en sí mismo se acumule y se intensifique", sin que se trate de una simple sumatoria de afectaciones aisladas²⁶.

Parte de ese daño acumulado consiste en el efecto disuasorio que la vigilancia genera, incluso sin que exista certeza de haber sido efectivamente vigilado. La Corte IDH sostuvo que la vigilancia o interceptación ilegítima de comunicaciones "puede generar, por sus efectos, una restricción directa o indirecta a la libertad de pensamiento y de expresión", dado el efecto

22 RELE (2025), Op. Cit., párr. 228, con cita a Corte IDH, CAJAR, párr. 542.

23 TEDH, *Klass y otros vs. Alemania* (1978), párr. 56; TEDH, *Roman Zakharov*, Op. Cit., párr. 233.

24 TEDH, Sección Cuarta, *Szabó y Vissy vs. Hungría* (2016), párrs. 71 y 81.

25 Relatoría Especial sobre los derechos a la libertad de reunión pacífica y de asociación, A/HRC/62/45, Op. Cit., párr. 112.g.

26 *Ibidem*, párrs. 105-107.

intimidatorio que produce la sola sospecha de que las comunicaciones no son confidenciales²⁷. La Relatora de protesta de ONU sostiene, en el mismo sentido, que los efectos disuasorios de la vigilancia "se producen cuando las personas modifican su comportamiento por temor a las consecuencias de un monitoreo real, insinuado o percibido", de modo que el daño no depende de que la vigilancia haya sido efectivamente confirmada. Esa incertidumbre, agrega, no es casual sino estructural: "la vigilancia digital remota e invisible genera una ambigüedad constante en torno a si la vigilancia está teniendo lugar", lo que obliga a las personas a "vivir suponiéndose vigiladas de manera constante"²⁸.

El daño acumulado, además, no se distribuye de forma pareja: la red internacional de organizaciones INCLO documentó que el impacto de la vigilancia digital se agrava en comunidades racializadas, mujeres, personas LGBTQ+ y otros grupos ya vulnerables, para quienes esta tecnología profundiza riesgos preexistentes de violencia y discriminación, que los impulsan a una mayor autocensura²⁹. Una evaluación de impacto que no incorpore esta dimensión interseccional subestima el daño real y deja fuera una parte central del daño que busca prevenir.

La Corte IDH constató empíricamente este efecto, con base en un peritaje psicosocial, en el caso CAJAR. Los integrantes de este Colectivo, abogados activistas, adoptaron actitudes de autocensura tras conocer las acciones ilícitas del organismo de inteligencia colombiano. A partir de ese hecho probado, la Corte concluyó que el efecto amedrentador "alcanzó colectivamente a todos quienes fueron objeto" de la vigilancia, no solo a quienes fueron efectivamente interceptados, por el "temor fundado" compartido³⁰. La Relatora de protesta de ONU documentó el mismo fenómeno a escala global: describe cómo periodistas de los Balcanes trataron a un colega cuyo dispositivo había sido "infectado con Pegasus" como si él mismo

27 Corte IDH, CAJAR, Op. Cit., párr. 626.

28 Relatoría Especial sobre los derechos a la libertad de reunión pacífica y de asociación, A/HRC/62/45, Op. Cit., párrs. 41 y 47 respectivamente.

29 Informes de Kenya Human Rights Commission (KHRC) y Defenders Coalition referidos en International Network of Civil Liberties Organisations (INCLO), *Submission to the UN Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*, párr. 249. Informe presentado para la 62.ª sesión del Consejo de Derechos Humanos de las Naciones Unidas, 2025.

30 Corte IDH, CAJAR, Op. Cit., párr. 628.

estuviera "literalmente infectado", generando exclusión de larga duración y problemas en su trayectoria profesional³¹.

4. Moratoria y/o prohibición de contratación y uso de *spyware* sin salvaguardas de derechos humanos

Con respecto específicamente a las tecnologías de *spyware*, la RELE recomienda a los Estados "establecer una moratoria sobre la compra, venta, transferencia y uso de todo tipo de software espía" hasta que implementen un marco regulatorio de derechos humanos³². En el mismo sentido, un grupo de Relatores de la ONU hizo un llamado conjunto en 2021 a que todos los Estados impusieran una moratoria global sobre la venta y transferencia de tecnología de vigilancia hasta contar con regulaciones robustas que garanticen su uso conforme a los estándares internacionales de derechos humanos, calificando de altamente peligroso e irresponsable permitir que el sector de la vigilancia opere como una zona libre de derechos humanos³³. Por su parte, la Relatora de protesta de ONU llega a una formulación aún más específica: propone directamente la prohibición de "el uso y la transferencia de herramientas digitales intrusivas que no respeten las garantías de derechos humanos, incluidos los programas espía altamente invasivos (cuyas funciones no puedan limitarse o cuyo uso no pueda ser objeto de una auditoría independiente)"³⁴. La Relatora de Contrterrorismo, por su parte, también abre la puerta a que los Estados evalúen que lo que corresponde es una prohibición permanente³⁵.

31 Relatoría Especial sobre los derechos a la libertad de reunión pacífica y de asociación, A/HRC/62/45, Op. Cit., párr. 57.

32 RELE (2025), Op. Cit., recomendación 13, pág. 92.

33 Comunicado conjunto de Relatores y Relatoras Especiales de la ONU "Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech", OHCHR, 12 de agosto de 2021.

34 Relatoría Especial sobre los derechos a la libertad de reunión pacífica y de asociación, A/HRC/62/45, Op. Cit., recomendación, párr. 112.i).i).

35 Relatoría Especial sobre la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo, A/HRC/52/39, Op. Cit., párr. 49.

II. DURANTE LA EJECUCIÓN DE LA MEDIDA

5. Control de exportaciones y registro obligatorio de proveedores de tecnología de vigilancia

El Alto Comisionado de las Naciones Unidas sostiene que los Estados deben adoptar regímenes de control de exportaciones que evalúen el marco legal del país de destino y el historial de derechos humanos del usuario final propuesto antes de autorizar la venta de tecnología de vigilancia³⁶. En este sentido, la RELE agrega que se debe prohibir la adquisición e importación de tecnologías comerciales de espionaje informático que carezcan de salvaguardas técnicas para limitar sus funciones a objetivos específicos, necesarios y proporcionales³⁷.

6. Respeto a los derechos humanos por diseño

Se trata de una especificación técnica exigible al diseño del software. Según entiende la Relatora de Contraterrorismo de ONU, para ser compatible con derechos humanos, el *spyware* debe, como mínimo, 1) permitir que la persona usuaria seleccione específicamente qué datos monitorear en lugar de acceder automáticamente a todo; 2) no acceder automáticamente a los datos de los contactos del objetivo; y 3) crear un registro de auditoría indeleble, permanente e inmodificable de cada acción tomada³⁸. Cualquier *spyware* que no reúna estas características, sostiene, "no puede ser compatible con los derechos humanos, por más regulado que esté de otro modo".

36 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OHCHR), *El derecho a la privacidad en la era digital — Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*, A/HRC/39/29, 3 de agosto de 2018, párr. 25.

37 RELE (2025), Op. Cit., recomendación 12, pág. 92.

38 Relatoría Especial sobre la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la lucha contra el Terrorismo, A/HRC/52/39, Op. Cit., Anexo, párr. 4.

7. Garantías sobre datos personales que no pueden ser objeto de excepción, ni siquiera por seguridad nacional

El Convenio 108+, protocolo modificadorio -próximo a entrar en vigencia- del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa ("Convenio 108"), estructura las excepciones a sus principios protectorios en tres regímenes, cada uno con facultades propias, según la finalidad perseguida. En este marco, el régimen aplicable a seguridad nacional y defensa exige que la excepción esté prevista por ley y constituya "una medida necesaria y proporcional en una sociedad democrática para cumplir ese fin"³⁹, pero deja a salvo un núcleo de disposiciones que ninguna excepción puede suprimir: la obligación de seguridad de los datos, los mecanismos de responsabilidad proactiva (*accountability*), y la garantía de que las decisiones de la autoridad de control sean apelables ante un tribunal. Y, de manera explícita, el propio art. 11.3 del Convenio condiciona cualquier excepción de seguridad nacional o defensa a que ese tratamiento de datos quede sujeto a "revisión y supervisión independiente y efectiva conforme a la legislación doméstica de la Parte".

Además, sobre la ley que habilita la excepción, agrega un estándar aplicable en particular al tratamiento encubierto o secreto: aunque no se exige hacer pública cada salvaguarda operativa aplicable a una actividad de tratamiento secreta, sí es necesario que la ley contenga "reglas claras" sobre el uso de esas excepciones, para cumplir con los requisitos cualitativos de accesibilidad y previsibilidad⁴⁰.

39 Comité Consultivo del Convenio 108 (T-PD), Consejo de Europa, *Guidelines on the general principles of Article 11 of the Modernised Convention 108*, T-PD(2021)7rev13, última revisión 19 de junio de 2025; sección 3. Se trata de una guía interpretativa oficial elaborada por el órgano técnico del Convenio 108 sobre las excepciones que admite su art. 11 (seguridad nacional, defensa, orden público, entre otras); no crea derechos ni obligaciones nuevas, sino que orienta la interpretación de una disposición ya vinculante para los Estados parte.

40 Comité Consultivo del Convenio 108 (T-PD), *Guidelines (...)*, Op. Cit., sección 4.1.

7.1 Protección reforzada de datos sensibles y de categorías específicas (periodistas, abogados, defensores de derechos humanos)

Los datos sensibles, como aquellos relativos a salud, vida sexual, creencias religiosas, afiliación sindical, datos biométricos, opiniones políticas, geolocalización, entre otros, constituyen una categoría de datos personales que exige protección especial porque "permiten calificar al individuo y ofrecen sustento para la elaboración de perfiles personales"⁴¹. Sobre esa base, la Corte IDH exige un deber reforzado de protección -como límite a la actividad de vigilancia- cuando las actividades alcanzan a abogados y periodistas por confidencialidad de fuentes y secreto profesional⁴².

Es importante aclarar que esta protección reforzada se extiende a defensores de derechos humanos en general, de manera amplia. La Corte IDH reconoció el "derecho a defender los derechos humanos" como un derecho autónomo⁴³, generando para el Estado un deber especial de protección sobre las personas defensoras (tanto abstenerse de estigmatizarlas u hostigarlas como garantizarles un entorno seguro). Esta protección reforzada debe extenderse a las actividades de vigilancia, teniendo en cuenta además que son muchas veces personas de estos colectivos quienes resultan sus objetivos.

Fue el caso, por ejemplo, del software espía Pegasus desplegado en México entre 2012 y 2018 contra al menos 25 objetivos, entre ellos defensores de derechos humanos, periodistas y miembros del Grupo Interdisciplinario de Expertos Independientes (GIEI) que investigó el caso Ayotzinapa⁴⁴. También se probó la presencia de los programas espía Pegasus y Circles en Kenia⁴⁵, al tiempo que se registraron múltiples casos de defensores de derechos humanos, periodistas y abogados sometidos a intentos de hackeo o vigilancia inexplicada: por ejemplo, activistas que participaron en protestas contra la brutalidad policial y la corrupción reportaron haber recibido enlaces sospechosos

41 Corte IDH, CAJAR, Op. Cit., párr. 554.

42 RELE (2025), Op. Cit., párr. 229, citando a CAJAR, párr. 555.

43 Corte IDH, CAJAR, Op. Cit., párr. 978. Este derecho contempla "la posibilidad efectiva de ejercer libremente, sin limitaciones y sin riesgos de cualquier tipo" las actividades de vigilancia, promoción, denuncia y defensa de derechos humanos.

44 RELE, *El impacto de la vigilancia (...)*, Op. Cit., párr. 11.

45 Informes de Citizen Lab (University of Toronto) y Privacy International referidos en *Ibíd.*, párr. 237.

o mensajes con malware previos a arrestos o hechos de intimidación⁴⁶.

7.2 Regulación del intercambio de información entre Estados

Cuando la legislación acepta el intercambio de información entre organismos de inteligencia del propio Estado o de otro, la regulación "debe precisar las condiciones para ello, los fines que habilitan el intercambio, las entidades autorizadas y las salvaguardas necesarias para la seguridad de la información"⁴⁷.

A su vez, el Convenio 108+ aporta un estándar de fondo aplicable específicamente a este tipo de transferencias: una Parte no puede transferir datos personales a otra jurisdicción salvo que exista un nivel de protección adecuado, y debe restringir la transferencia cuando exista "un riesgo real y grave" de que sirva para eludir las garantías del Convenio (art. 14.1 y 14.2). Es un dato relevante que las excepciones por seguridad nacional y defensa previstas no alcanzan a estos dos límites, de modo que el núcleo de esta protección en materia de transferencias transfronterizas sigue rigiendo incluso cuando el intercambio de información ocurre entre organismos de inteligencia de distintos Estados.

Por otro lado, es interesante reponer que la RELE-CIDH documenta, desde el ángulo inverso, el costo de no tener mecanismos robustos en este punto: el carácter transnacional de las operaciones de vigilancia "ha creado lagunas jurisdiccionales que agravan aún más la impunidad", dejando a las víctimas sin posibilidad de exigir responsabilidades más allá de las fronteras⁴⁸.

46 Informes de Kenya Human Rights Commission (KHRC) y Defenders Coalition referidos en International Network of Civil Liberties Organisations (INCLO), Op. Cit., párr. 238.

47 Corte IDH, CAJAR, Op. Cit., párr. 539.

48 RELE (2025), Op. Cit., párr. 273.

III. UNA VEZ FINALIZADA LA MEDIDA

8. Supervisión en tres etapas: autorización previa, control durante la medida y examen ex post

Es principalmente el TEDH quien sistematiza este esquema, entendiendo que la revisión y supervisión de medidas de vigilancia secreta debe estar presente cuando la medida se ordena por primera vez (autorización previa e independiente cuando se define el objeto y alcance), mientras se ejecuta, y después de terminada⁴⁹.

9. Mecanismos de supervisión con independencia estructural y decisiones vinculantes

Según el derecho internacional, el marco jurídico interno debe establecer instituciones de control que sean estructuralmente independientes del Poder Ejecutivo y, en su caso, de los servicios de inteligencia y/o fuerzas de seguridad. Deben tener conocimientos técnicos y acceso directo y completo a la información, y dedicarse a fiscalizar el cumplimiento normativo, la eficiencia, la situación financiera y los métodos administrativos de quienes despliegan estas técnicas⁵⁰.

No alcanza con que exista únicamente de manera formal una vía de reclamo frente a una medida de vigilancia. El TJUE invalidó el mecanismo de protección a través de un Defensor ("Ombudsperson") previsto en el acuerdo "Privacy Shield" entre EE.UU. y la UE para la transferencia de datos señalando que no estaba garantizada su independencia frente al Poder Ejecutivo ni que tuviera la facultad de tomar decisiones vinculantes para -en ese caso- los servicios de inteligencia⁵¹. El Tribunal fijó así un test de dos elementos para evaluar si cualquier mecanismo de supervisión o reclamo es una salvaguarda genuina

49 TEDH, *Roman Zakharov*, Op. Cit., párr. 233 y *Big Brother Watch*, Op. Cit., párr. 350.

50 Corte IDH, *CAJAR*, Op. Cit., párr. 564.

51 Tribunal de Justicia de la Unión Europea (TJUE), *Schrems II*, C-311/18, 16 de julio de 2020, párrs. 195-197.

o solo nominal: 1) que su independencia esté garantizada por reglas estructurales, no solo por la práctica; y 2) que tenga poder de dictar decisiones vinculantes sobre el organismo controlado, no solo de emitir recomendaciones.

En algunos casos se recomienda también la creación de una institución civil, adicional al control judicial. Por ejemplo, cuando las medidas de vigilancia fueron dictadas en el marco de investigaciones judiciales: el TEDH sostiene que esto es necesario en tanto el juez que dictó la orden de vigilancia "no está en condiciones de garantizar una supervisión eficaz" por sí solo⁵². Por su lado, la RELE recomienda la existencia de una "autoridad civil independiente de supervisión", con mandato que incluya expresamente la consideración de los procesos de vulnerabilidades equitativas (es decir, si el Estado divulga o retiene vulnerabilidades de software recién descubiertas)⁵³.

10. Notificación y ejercicio de derechos

Según distintos órganos de Naciones Unidas, es indispensable reconocer el derecho de las personas a ser notificadas de que fueron objeto de una medida de vigilancia una vez que esta finalizó y ya no existe riesgo para la investigación en curso⁵⁴.

Esto forma parte del derecho de toda persona a ejercer su autodeterminación informativa -que la Corte IDH reconoce como un derecho humano autónomo-: poder conocer qué datos existen sobre su persona y cómo fueron obtenidos, rectificarlos, solicitar su eliminación cuando la recopilación fue ilegal y/u oponerse a su tratamiento si lo deseara⁵⁵.

52 TEDH, *Roman Zakharov*, Op. Cit., párr. 274 y TEDH, Sección Cuarta, *Ekimdzhiyev y otros vs. Bulgaria* (2022), párr. 349.

53 RELE (2025), Op. Cit., párrs. 231 y 236.

54 OHCHR, A/HRC/27/37, Op. Cit., párrs. 39-41 y, en el mismo sentido, Relatoría Especial sobre los derechos a la libertad de reunión pacífica y de asociación, A/HRC/62/45, Op. Cit., párr. 25, con cita a jurisprudencia del TEDH.

55 Corte IDH, *CAJAR*, Op. Cit., párrs. 585-586.

10.1 Recurso efectivo y ejercicio de derechos sobre datos personales

En este sentido, debe existir un mecanismo de exigibilidad de este derecho, para que las personas afectadas puedan efectivamente conocer si fueron objeto de actividades arbitrarias de vigilancia o inteligencia y, en su caso, disponer sobre esos datos y acceder a reparaciones por usos ilegítimos. Se entiende como parte de la reparación integral el suministro de información completa sobre el alcance y la duración de la medida, y "la destrucción de los datos obtenidos ilegalmente"⁵⁶, y la posibilidad de compensación por daños. Esto debe poder materializarse a través de un recurso judicial efectivo, cuyas decisiones sean ejecutables⁵⁷.

En este sentido, cuando una normativa no prevé ninguna vía legal para que la persona acceda, rectifique o suprima sus propios datos, esa ausencia vulnera la esencia misma del derecho a la tutela judicial efectiva. El TJUE entendió a la falta de recurso como una violación tan grave como la vigilancia misma. Sostuvo que una normativa que permite a las autoridades públicas acceder "con carácter generalizado" al contenido de las comunicaciones electrónicas vulnera el contenido esencial del derecho a la vida privada⁵⁸. Y, en un paso adicional, sostuvo que una normativa que no prevé "ninguna posibilidad" de que la persona ejerza vías legales para acceder a sus datos personales, u obtener su rectificación o supresión, "no respeta la esencia" del derecho fundamental a la tutela judicial efectiva⁵⁹. Algunos años después, el TJUE consolidó el estándar más exigente que el "derecho a un recurso", reforzando que no se trata de un mecanismo en abstracto sino de una condición de existencia del derecho mismo⁶⁰.

Esta exigencia es particularmente relevante teniendo en cuenta que, según informes recientes, nuestra región muestra un patrón sistemático de incumplimiento. La RELE concluyó que "ningún Estado de las

56 RELE (2025), Op. Cit., párrs. 271 y 272.

57 Corte IDH, *CAJAR*, Op. Cit., párr. 565 con base en el art. 25 de la CADH.

58 TJUE, *Schrems I*, C-362/14, 6 de octubre de 2015, párr. 94.

59 *Ibidem*, párr. 95.

60 TJUE, *Schrems II*, Op. Cit., párrs. 191 y 192.

Américas (...) ha proporcionado un recurso significativo a las víctimas"⁶¹. El caso mexicano de la FEADLE (Fiscalía Especial para la Atención de Delitos cometidos contra la Libertad de Expresión) ilustra en concreto este escenario: las denuncias de víctimas de Pegasus derivaron en que "las investigaciones sobre los abusos de vigilancia se han convertido en investigaciones de las víctimas, en lugar de los autores"⁶². Es decir que el recurso existía formalmente, pero en la práctica terminó por revictimizar a quienes fueron objeto de estas acciones y decidieron reclamar, en vez de a quien desplegó la tecnología.

11. Transparencia y registro del uso de tecnologías de vigilancia

La doctrina es clara en que los Estados deben ser "completamente transparentes respecto del uso y alcance" de los poderes de vigilancia, publicando como mínimo información agregada sobre solicitudes aprobadas y rechazadas, desagregadas por proveedor de servicios⁶³. En particular, RELE fija un estándar mínimo de información pública para el control ciudadano que incluye la divulgación de contratos gubernamentales, un registro de proveedores y la revelación de las herramientas adquiridas y sus especificaciones⁶⁴.

La Corte IDH va un paso más allá y puntualiza que el despliegue de este tipo de medidas debe formalizarse mediante "procesos numerados", con registro de todas sus etapas, incluido el historial de accesos a sistemas electrónicos; para el tratamiento de datos personales, el registro debe identificar responsables, propósitos, base jurídica, plazos de conservación y técnicas utilizadas⁶⁵.

61 RELE, *El impacto de la vigilancia* (...), Op. Cit., párrs. 269 y 270.

62 RELE-CIDH, *El impacto de la vigilancia digital en la libertad de expresión en las Américas*, Op. Cit., párr. 130, con cita a la organización mexicana R3D - Red en Defensa de los Derechos Digitales.

63 OHCHR, A/HRC/27/37, Op. Cit., párr. 40.

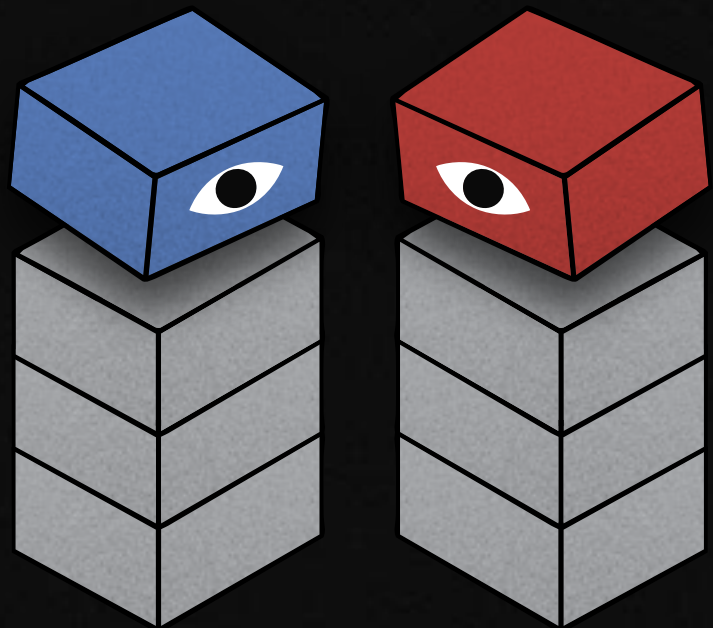
64 RELE (2025), Op. Cit., párr. 234.

65 Corte IDH, *CAJAR*, Op. Cit., párr. 540.

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

CONCLUSIÓN

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



CONCLUSIÓN

El relevamiento muestra una convergencia significativa entre los tres sistemas de protección de derechos humanos trabajados (universal, interamericano y europeo) en torno a un núcleo de exigencias que abarca todo el ciclo de despliegue de tecnologías intrusivas por parte de los Estados.

Antes de su utilización, es preciso verificar la legalidad, necesidad y proporcionalidad de manera estricta, dado que sus capacidades técnicas son especialmente intrusivas. En particular, el requisito de legalidad exige una base normativa pública, que habilite el despliegue únicamente para fines taxativos y no discriminatorios. A eso se suma la exigencia de autorización judicial previa e individualizada, una evaluación de impacto integral y, en el caso específico del *spyware*, un régimen de moratoria o incluso de prohibición mientras no existan garantías suficientes de respeto a los derechos humanos.

Estas garantías deben sostenerse durante la ejecución de la medida, mediante controles estrictos, diseños de tecnologías respetuosas de los derechos humanos, salvaguardas sobre datos personales y, en particular, protección reforzada sobre grupos especialmente vulnerables, que suelen ser objeto de vigilancia.

Por último, una vez finalizada la medida, debe haber supervisión a cargo de instituciones independientes y con capacidad de dictar decisiones vinculantes y registros públicos del uso de la tecnología. A la vez, se debe notificar a quienes hayan sido objeto de vigilancia, reconociendo su derecho a la autodeterminación informativa y, cuando la actividad fue ilegítima, garantizar un recurso judicial efectivo.

La convergencia entre los distintos sistemas le da peso a estos estándares más allá de la fuente puntual que los enuncia en cada caso. Al mismo tiempo, el relevamiento deja algo claro: el *spyware* no es una modalidad más de vigilancia estatal a la que baste con aplicarle, sin más, los estándares desarrollados para la interceptación de comunicaciones tradicional. Por su capacidad de acceso total al dispositivo intervenido, exige un escrutinio reforzado en el análisis de necesidad y proporcionalidad, y una atención particular a los efectos que produce incluso antes de traducirse en una violación puntual y comprobable.

El respeto a principios generales o criterios mínimos, como los que relevamos en este documento, es fundamental por el tipo de impacto que tiene el uso de tecnologías de este tipo. Vimos que el efecto disuasorio que genera la vigilancia alcanza colectivamente a quienes fueron objeto de la medida y a su entorno, incluso cuando no hay certeza de haber sido efectivamente vigilados, y ese daño se acumula sobre múltiples derechos a la vez, reforzando el impacto en comunidades ya vulnerables. A esto se suma una asimetría que distingue a esta tecnología de otras formas de injerencia estatal: por su propio diseño encubierto, quien es vigilado rara vez puede saberlo, lo que vuelve insuficiente cualquier exigencia pensada únicamente para el momento posterior al daño. Es, por esto, más difícil de contrarrestar por vías puramente reactivas, y de ahí la relevancia de exigir estos estándares de manera preventiva, en cada uno de los tres momentos trabajados en este documento.

