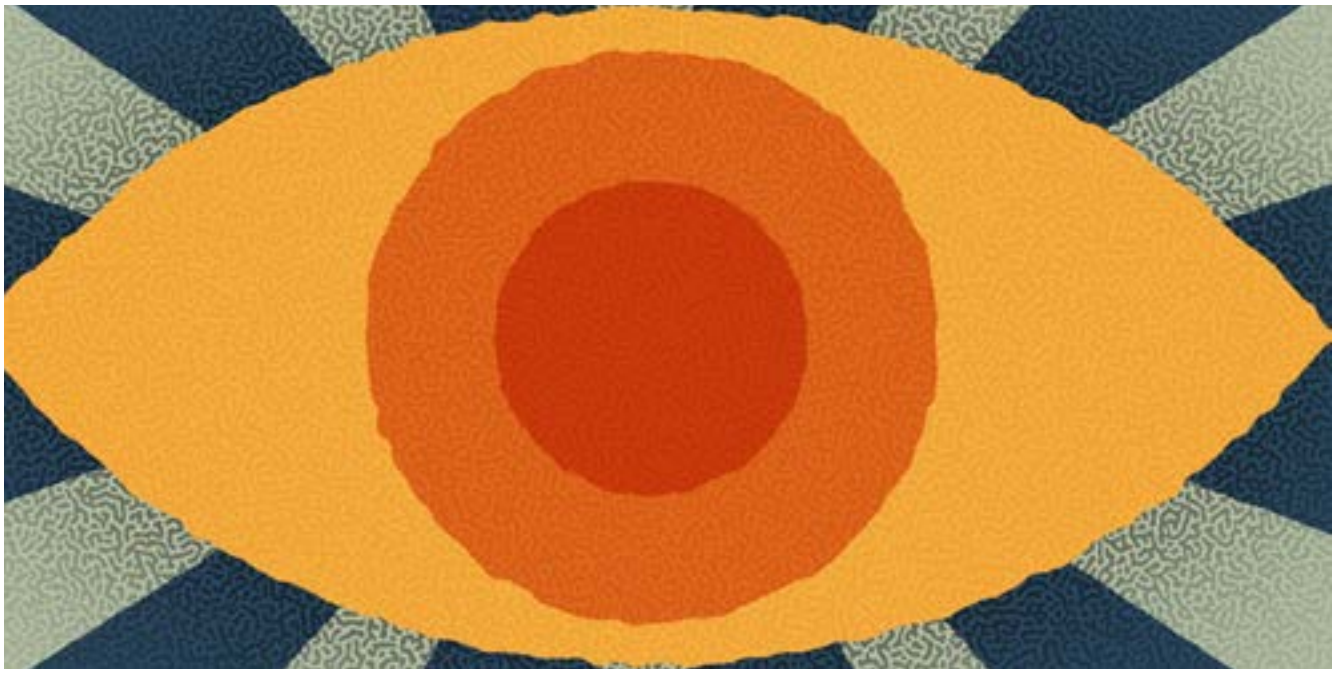

Enfrentando la vigilancia digital arbitraria en las Américas

Garantías esenciales y medidas institucionales para que las actividades de seguridad del Estado respeten los derechos a la privacidad y a la información

VERIDIANA ALIMONTI
Directora Asociada de Politicas en América Latina

Mayo 2026

ELECTRONIC FRONTIER FOUNDATION

Autora: Verdiana Alimonti

Una publicación de la Electronic Frontier Foundation, 2026.

Paige Collings, activista sénior de libertad de expresión y privacidad de la EFF, ha revisado esta guía. David Greene, asesor jurídico sénior de la EFF, ha revisado su contenido. Kim Carlson, directora de diseño de la EFF, se ha encargado del formato de esta guía. Carlos Wertheman, director sénior de traducciones de la EFF, la ha traducido al español. Consulta este informe en línea: https://www.eff.org/wp/tackling-arbitrary-digital-surveillance-americas?language=es

CONTENTS

INTRODUCCIÓN

En todas las Américas, la escasa rendición de cuentas, los débiles mecanismos de control y los marcos jurídicos insuficientes dan lugar constantemente a violaciones de los derechos humanos en el contexto de la seguridad pública, la aplicación de la ley y las actividades de inteligencia. El aumento de las capacidades de vigilancia digital es un elemento central de los abusos actuales, como la capacidad de perfilar y clasificar a las personas; vigilar sus movimientos, relaciones y rutinas; intervenir en diferentes tipos de comunicaciones; e inferir o supuestamente predecir comportamientos con consecuencias perjudiciales para las personas.

En respuesta a ello, la Electronic Frontier Foundation ha elaborado esta guía centrada en la privacidad y la protección de datos, así como en garantías de acceso a la información, con el fin de proporcionar orientación concreta y aplicable a los gobiernos de las Américas para frenar el círculo vicioso de los abusos de la vigilancia digital estatal. Este documento describe qué salvaguardias y medidas institucionales deben estar en vigor para proteger a las personas en toda la región, y detalla las normas, los parámetros y los estándares establecidos en el Sistema Interamericano de Derechos Humanos como aportación para superar las prácticas y tendencias perniciosas actuales. Si bien señala las garantías esenciales necesarias, no pretende ser exhaustiva ni excluir otras medidas importantes que no se mencionan explícitamente en estas páginas.

Esta guía se basa en un marco jurídico integral relativo a la protección de las personas frente a la vigilancia digital estatal y las actividades relacionadas con la seguridad. Las conclusiones recientes de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos («CIDH», «Comisión Interamericana» o «Comisión») señalaron que:

> *«Las tecnologías de vigilancia digital se han convertido en una amenaza sistémica para los derechos humanos en todo el hemisferio, alterando de manera fundamental la relación entre los Estados y sus ciudadanos. La evidencia presentada en este informe demuestra que las prácticas de vigilancia que antes se consideraban excepcionales en virtud del derecho internacional de los derechos humanos se han normalizado cada vez más, creando un entorno permisivo para la violación continua de los derechos fundamentales».*

El Relator Especial hizo hincapié en que el carácter sistémico de la vigilancia en toda la región pone de manifiesto lagunas fundamentales en los marcos jurídicos, los mecanismos de supervisión y los sistemas de rendición de cuentas que deben abordarse de manera integral. Como señaló el Relator, el resultado no es solo la violación de los derechos individuales, sino la erosión sistemática de las instituciones democráticas y el Estado de Derecho.

Hace más de una década, el informe de la Comisión Interamericana sobre seguridad ciudadana y derechos humanos también hizo hincapié en los derechos humanos como límites esenciales para impedir que las facultades otorgadas por ley a los agentes del Estado para defender la seguridad de todos sean, por el contrario, utilizadas por las fuerzas de seguridad para avasallar derechos. Por lo tanto, las garantías consagradas en la Convención Americana sobre Derechos Humanos sirven de guía para las actividades de las fuerzas de seguridad en el cumplimiento de los derechos humanos.

Además, la Corte Interamericana de Derechos Humanos («Corte Interamericana» o «Corte») ha interpretado la Convención para establecer parámetros cruciales para el cumplimiento de los derechos y principios convencionales frente a la vigilancia estatal. En particular, la sentencia de la Corte en el Caso Miembros de la Corporación Colectivo de Abogados « José Alvear Restrepo» vs. Colombia (*CAJAR vs. Colombia*) profundizó en las garantías convencionales para establecer normas y criterios fundamentales que aseguren los derechos a la privacidad y a la información en las acciones de seguridad del Estado. Si bien este caso aborda más específicamente las actividades de inteligencia, las salvaguardias que establece la sentencia constituyen una base fundamental para la vigilancia digital estatal y las actividades relacionadas con la seguridad en un sentido más amplio.

Otras tres referencias importantes, dado el alcance de esta guía, son los Principios Necesarios y Proporcionados sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones, la Recopilación de buenas prácticas para garantizar los derechos humanos por los servicios de inteligencia y los Principios de Tshwane sobre seguridad nacional y el derecho a la información. A lo largo del

documento destacamos conexiones relevantes con los Principios Necesarios y Proporcionados, que los lectores deben tener en cuenta junto con esta guía.[1]

La adopción de medidas concretas para aplicar lo que sigue no debe considerarse un acto de buena voluntad, sino un deber de los Estados en virtud de sus compromisos con el derecho internacional de los derechos humanos.

1. Protecciones a la privacidad de los datos en la Convención Americana sobre Derechos Humanos

El derecho a la vida privada tiene un alcance amplio en virtud de la Convención Americana. **El artículo 11 prohíbe toda injerencia arbitraria o abusiva en la vida privada de una persona, incluida la intimidad de su familia, su hogar, su correspondencia y sus comunicaciones**. Esta protección abarca tanto el contenido de lo que las personas comunican como los metadatos que se derivan del proceso de comunicación o interacción digital.

La protección de la vida privada está directamente relacionada con la salvaguarda de la autonomía personal, el desarrollo personal y el derecho a establecer relaciones con otras personas y con el mundo exterior. El alcance de la información que las instituciones conocen sobre una persona y la forma en que procesan dichos datos puede afectar profundamente el curso de la vida de una persona y sus interacciones sociales.

En este sentido, la Corte destacó que la vida privada comprende la forma en que la persona se ve a sí misma y cómo decide proyectarse hacia los demás. Tiene una conexión intrínseca con la dignidad y la autodeterminación, defendiendo la capacidad de las personas para elegir libremente las opciones y circunstancias que dan sentido a su existencia en función de sus preferencias, valores y convicciones.

En consecuencia, la Corte destacó que la autodeterminación abarca la libertad de las personas para decidir cuándo y en qué medida revelar aspectos de su vida privada, incluido el tipo de información que otros pueden conocer sobre ellas. La sentencia *CAJAR vs. Colombia* señaló específicamente la importancia de estas garantías para salvaguardar los derechos de los niños, destacando la privacidad como un factor determinante para el pleno desarrollo de su personalidad y su vida futura.

1 Los 13 principios son: legalidad, objetivo legítimo, necesidad, idoneidad, proporcionalidad, autoridad judicial competente, debido proceso, notificación del usuario, transparencia, supervisión pública, integridad de las comunicaciones y sistemas, garantías para la cooperación internacional y garantías contra el acceso ilegítimo y derecho a recurso efectivo.

Sin embargo, el derecho a la vida privada no es un derecho absoluto y puede ser limitado siempre que las injerencias no sean abusivas o arbitrarias. Para ello, las injerencias admisibles deben estar debidamente establecidas en la ley, perseguir un fin legítimo y ser adecuadas, necesarias y proporcionadas en una sociedad democrática para cumplir objetivos legítimos específicos. Esto se conoce como la «prueba de las tres partes».

El cumplimiento de estos requisitos implica un conjunto fundamental de pasos, medidas y salvaguardias que la Corte Interamericana, la Comisión Interamericana y la Relatoría Especial para la Libertad de Expresión han destacado, y que esbozamos a continuación.

2. Garantías fundamentales de privacidad en el marco de la vigilancia digital estatal

Citando al Tribunal Europeo de Derechos Humanos, la sentencia de la Corte Interamericana en el caso *CAJAR vs. Colombia* reiteró que la mera existencia de legislación que permita un sistema de seguimiento secreto de las comunicaciones de las personas implica una injerencia en el derecho a la privacidad. También afecta al derecho a la libertad de pensamiento y de expresión, ya que el derecho a la privacidad está profundamente interrelacionado con el libre desarrollo e intercambio de ideas.

La Relatoría Especial para la Libertad de Expresión de la CIDH subrayó la urgente necesidad, en las Américas, de contar con mecanismos integrales para prevenir los abusos de vigilancia antes de que se produzcan, detectarlos cuando ocurran y proporcionar recursos efectivos a las víctimas y sanciones a los agentes responsables.

Las salvaguardias necesarias para frenar la vigilancia digital abusiva abarcan leyes con límites y definiciones claros, medidas de protección basadas en un análisis sólido, necesario y proporcionado, controles concretos y una supervisión independiente con facultades robustas.

LA CAJA NEGRA DE LOS ABUSOS DE LAS FUERZAS DE INTELIGENCIA

Aunque la vigilancia estatal suele estar envuelta en el secreto, existe una mayor tendencia a ocultar información de interés público —como normativas, protocolos, estadísticas, gastos presupuestarios y tecnologías en uso— cuando esta se refiere a organismos o actividades de inteligencia. Además, saber que se ha sido objeto de vigilancia por parte de los servicios de inteligencia, incluso una vez que han cesado

las investigaciones o las sospechas, resulta mucho más difícil, si no imposible. La sentencia de la Corte en el caso *CAJAR vs. Colombia* reviste especial importancia por subrayar que las actividades de inteligencia no quedan al margen de las obligaciones en materia de derechos humanos, y por especificar tanto su alcance como el criterio de legitimidad.

La sentencia **define las actividades de inteligencia** en términos generales como acciones destinadas a obtener, analizar y difundir información para apoyar la toma de decisiones por parte de las entidades responsables de implementar políticas de seguridad. Distingue las tareas de los organismos de inteligencia de las propias de la seguridad pública, haciendo hincapié en el mayor riesgo de arbitrariedad y de violación de los derechos humanos cuando una misma institución lleva a cabo ambos tipos de tareas. En este sentido, los servicios de inteligencia no deben tener facultades de arresto, detención y el ejercicio de potestades con alcance coercitivo sobre las personas, como la investigación criminal.[2]

Los organismos de inteligencia tampoco deben llevar a cabo investigaciones previas al juicio, lo que implicaría la erosión de las garantías del debido proceso. Si bien tanto las investigaciones penales como las operaciones de inteligencia tienen por objeto encontrar y procesar información, y ambas pueden compartir métodos para recabar y analizar datos, persiguen fines esencialmente diferentes. Los servicios de inteligencia operan con una función preventiva, no de represión directa del delito.

Como señala la Corte, dicha función preventiva tiene por objeto la seguridad y la protección de la sociedad y de las personas. Establece claramente **cuál debe ser el objetivo último de las actividades de inteligencia:** «[estas] necesariamente deben conducirse con el objetivo último de proteger a las personas que habitan en el territorio del Estado, lo que incluye la salvaguarda de sus derechos y libertades». Por lo tanto, las múltiples tareas que implican estas actividades solo son útiles y necesarias en la medida en que sirvan para satisfacer este objetivo fundamental. Por el contrario, si las acciones de inteligencia ponen en peligro sistemáticamente la vida y las libertades de las personas, persiguen y tratan de acallar las críticas, o ponen en peligro de cualquier otra forma los derechos de las personas y las sociedades democráticas, entonces carecen de su fundamento legítimo principal y no son compatibles con el derecho internacional de los derechos humanos.

---

2 En relación con ello, la Comisión Interamericana hizo hincapié en que los Estados deben establecer una clara distinción, en su marco jurídico interno, entre las funciones de defensa nacional, a menudo desempeñadas por las fuerzas armadas, y las de seguridad ciudadana, a cargo de las fuerzas policiales. Teniendo en cuenta la naturaleza de cada fuerza y los antecedentes negativos de la región en relación con la intervención militar en asuntos de seguridad interna, las funciones vinculadas a la prevención, la disuasión y la represión legítima de la violencia y del delito corresponden exclusivamente a las fuerzas policiales, bajo la dirección superior de las autoridades legítimas de un gobierno democrático. CIDH, Informe sobre Seguridad Ciudadana y Derechos Humanos, 2009, Recomendaciones específicas (B), punto 10. Disponible en https://hchr.org.mx/publicaciones/nforme-sobre-seguridad-ciudadana-y-derechos-humanos-2009/

2.1. Marco jurídico claro y preciso

Cualquier limitación a la privacidad y a sus garantías conexas debe estar prescrita por la ley, promulgada por el poder legislativo y accesible al público. De este principio básico se derivan algunas orientaciones importantes:

- El marco jurídico que autoriza y regula la vigilancia estatal, incluidas las actividades de inteligencia, nunca puede ser de carácter reservado.
- La ley debe definir el alcance de las actividades de vigilancia, los fines que por su medio deben perseguirse y las facultades de los órganos y autoridades competentes de manera clara y precisa, de modo a permitir que las personas tengan conocimiento previo de su aplicación y puedan preverla (véase *3. Transparencia y participación*).
- Las protecciones legales sólidas deben seguir el ritmo de los avances tecnológicos, y las revisiones periódicas deben ser el resultado de un proceso legislativo o regulatorio participativo.

La Corte afirmó que las leyes de inteligencia deben establecer, con la mayor precisión posible: las distintas amenazas que determinan la necesidad de emprender actividades de inteligencia, junto con una especificación clara y exhaustiva de las facultades otorgadas a los agentes estatales que llevan a cabo estas actividades. Las amenazas establecidas en la legislación nacional deben referirse a factores o situaciones que, considerados de manera racional y concreta, puedan poner en peligro la realización de los fines legítimos. La ley debe indicar, por tanto, tanto los fines legítimos como las posibles amenazas específicas contra ellos (véase *2.2. Fines legítimos*).

La legislación nacional debe proporcionar también un «sistema bien definido y completo para autorizar, vigilar y supervisar las actividades de inteligencia en situaciones concretas». Basándose en las acciones y estrategias de inteligencia para obtener y recopilar información, dicha legislación debe establecer, con la mayor precisión posible:

- los tipos de medidas y acciones de obtención y análisis de información autorizadas en materia de inteligencia;
- los objetivos perseguidos que justifican estas medidas;
- las clases de personas y actividades respecto de las cuales los agentes pueden obtener y recopilar información, siempre basándose en la identificación de amenazas a fines legítimos previamente identificados;
- el grado de sospecha que justifique el uso de medidas de obtención y

recopilación de información, siguiendo criterios de necesidad y proporcionalidad;

- los plazos para la ejecución de las medidas y estrategias de recopilación de información; y
- los métodos para autorizar, supervisar y examinar dichas medidas y acciones.

Si la legislación nacional autoriza **el intercambio de información entre organismos de inteligencia y seguridad nacionales o extranjeros,** también debe establecer parámetros claros para dicho intercambio, incluidos los fines que habilitan el intercambio, las entidades autorizadas y las salvaguardias aplicables.

Las siguientes secciones sobre «fines legítimos», «idóneo, necesario y proporcionado» y «garantías adicionales para el tratamiento de datos personales» detallan aspectos importantes sobre cómo la legislación nacional debe considerar o abordar determinados conceptos y disposiciones requeridas.

2.2. Fines legítimos

Las actividades de las fuerzas de seguridad deben perseguir fines que sean legítimos y necesarios en una sociedad democrática. Esta condición se aplica a las operaciones de vigilancia estatal y a la forma en que estas interfieren con la privacidad y la protección de datos. En general, la Convención Americana considera fines legítimos los de preservar la seguridad nacional, mantener el orden público, salvaguardar la salud pública y proteger los derechos humanos.

Sin embargo, en la sentencia *CAJAR vs. Colombia*, **la Corte destacó los peligros de utilizar nociones vagas e imprecisas para justificar las acciones de inteligencia, y aclaró algunos aspectos importantes para delimitar el alcance de los fines legítimos.** Por ejemplo, preservar la seguridad nacional puede implicar la protección de la propia existencia del Estado, su integridad territorial o su independencia política frente a amenazas específicas y definidas. A su vez, la protección de los derechos humanos debe referirse a situaciones que constituyan un riesgo concreto para el goce efectivo o la garantía de determinados derechos.

Una evaluación fundamental para cualquiera de los fines legítimos que menciona la Convención es su conexión con la defensa de las sociedades democráticas. Como señaló la Corte:

> *«Los objetivos antes mencionados se revelan como "fines legítimos" en función de su correspondencia con el fin que, a la postre, fundamenta y guía la existencia de un Estado de Derecho, es decir (...) 'la protección de los derechos esenciales [de la persona humana] y la creación de circunstancias que le permitan progresar espiritual y materialmente'».*

Esto se relaciona con lo que hemos señalado anteriormente en relación con las actividades de inteligencia, y que se aplica en términos generales a las fuerzas de seguridad del Estado: su finalidad última, en virtud del derecho internacional de los derechos humanos, es proteger a las personas, sus derechos y libertades dentro de una sociedad democrática. **Si las prácticas de seguridad del Estado se desvían de ello, entonces constituyen una amenaza para lo que se supone que deben proteger, y deben abordarse como un ejercicio ilegítimo y abusivo del poder**.

De ello se desprenden dos conclusiones cruciales e interrelacionadas:

- En primer lugar, los objetivos legítimos **prohíben cualquier actividad de seguridad con fines discriminatorios**[3] por razones de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social. Las operaciones de inteligencia no deben tener como objetivo promover, beneficiar o afectar a una determinada actividad, persona o grupo basándose en dichos atributos.
- En segundo lugar, los organismos de seguridad **no deben llevar a cabo actos tendientes a neutralizar, perseguir o atacar a la oposición o a quienes expresan opiniones discrepantes**. El pluralismo político es fundamental para la democracia, un valor que sustentan los artículos 13, 16 y 26 de la Convención Americana.

2.3. Idóneo, necesario y proporcionado

Cualquier operación de vigilancia digital por parte de las fuerzas de seguridad del Estado debe ser necesaria en una sociedad democrática. Esto implica un test de proporcionalidad basado en criterios que deben especificarse adecuadamente en la legislación nacional. **Las autoridades competentes deben llevar a cabo este análisis antes de autorizar o implementar tareas de vigilancia en casos concretos, incluso como parte de actividades de inteligencia**.

El análisis debe considerar la base jurídica que sustenta las actividades de vigilancia, los fines legítimos específicos que persiguen y si cumplen las siguientes condiciones:

- la vigilancia es adecuada para hacer frente a amenazas o daños específicos a los fines legítimos;
- la vigilancia no es solo útil, sino estrictamente necesaria, y las acciones o métodos

3 Para más información sobre las normas interamericanas en materia de igualdad y no discriminación, véase www.eff.org/document/human-rights-standards-government-use-ai-latin-america-appendix (apartado 4.3. Igualdad y no discriminación).

concretos empleados son esenciales para hacer frente a amenazas o daños específicos a los fines legítimos, lo que significa que no existe una alternativa viable y menos gravosa capaz de alcanzar el mismo objetivo;

- las medidas de vigilancia son estrictamente proporcionadas, es decir, el sacrificio inherente a la restricción de derechos no devenga exagerado ni desmedido en relación con el beneficio de salvaguardar fines legítimos específicos en el caso concreto.

La facultad de autorizar medidas de vigilancia digital recae en la autoridad judicial, que debe llevar a cabo rigurosamente el análisis de proporcionalidad (véase *2.4.(i) Orden judicial previa*).

Estos requisitos están en consonancia con los principios 3, 4 y 5 de los Principios Necesarios y Proporcionados sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones, que aportan orientaciones críticas adicionales. Entre otras cosas, es importante que:

- La información a la que se acceda se limite a lo que sea relevante y material para la amenaza o el delito grave, y que no se conserve la información excedente recopilada.
- Solo las autoridades competentes especificadas tengan acceso a la información y la utilicen únicamente para los fines y durante el tiempo autorizados por la autoridad judicial.

2.4. Controles esenciales

(i) Orden judicial previa

Según la Corte, **la protección efectiva de la privacidad y la libertad de pensamiento y de expresión requiere una orden judicial previa para cualquier medida de vigilancia de las comunicaciones**. También es obligatorio, como regla general, obtener una autorización judicial adecuada para el allanamiento al domicilio o de locales privados.

Como la Corte ejemplificó ampliamente en el caso *CAJAR vs. Colombia*, **las medidas de vigilancia de las comunicaciones y digital que requieren una orden judicial previa abarcan** la interceptación, cualquier tipo de monitoreo o vigilancia de las comunicaciones —ya sea por teléfono, transmisión de datos u otras redes—, la grabación electrónica, incluida la audiovisual, la recopilación de datos en poder de particulares o empresas, así como el acceso a bases de datos y sistemas de información no públicos que almacenan y procesan información personal, el rastreo

de usuarios en la red o la localización de dispositivos electrónicos. En este sentido, la Corte señaló que las técnicas o métodos para obtener acceso a metadatos y datos telemáticos sensibles, tales como el correo electrónico, y metadatos de aplicaciones «Over the Top», datos de localización, direcciones IP, estación de torre celular, nubes de datos, GPS y Wi-Fi requerirían una orden judicial previa.

Las actuales tecnologías de vigilancia digital son capaces de procesar una cantidad dispersa y masiva de datos, lo que facilita y agiliza la categorización y la elaboración de perfiles de personas y grupos, con un impacto significativo en sus vidas. La necesidad de reforzar la protección de los datos personales sensibles pone de relieve lo esenciales que son las órdenes judiciales para autorizar la vigilancia digital.

La Corte destacó que **los datos personales sensibles** afectan a «los aspectos más íntimos de las personas» y pueden incluir datos relacionados con la salud personal de un individuo, su vida sexual u orientación sexual, sus creencias religiosas, filosóficas o morales, su afiliación sindical, datos genéticos, datos biométricos dirigidos a identificar de manera única a una persona física, opiniones políticas, origen racial o étnico, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños y niñas o geolocalización personal.

La labor de periodistas y abogados también requiere un nivel reforzado de protección en lo que respecta a las operaciones de vigilancia. La Corte señaló que es imperativo limitar las actividades de inteligencia para salvaguardar el secreto de las fuentes de los periodistas y proteger la confidencialidad de todas las comunicaciones entre abogados y sus clientes en el marco de su relación profesional.

La Corte hizo hincapié en que exigir autorización judicial para la vigilancia digital es coherente con el rol de las juezas y los jueces como garantes de los derechos humanos en un sistema democrático. La autoridad judicial debe ser independiente y, como tal, capaz de garantizar una supervisión objetiva de otras entidades y autoridades públicas en lo que respecta al cumplimiento de la ley.[4]

Como señaló la Corte, la autoridad judicial es la encargada de evaluar, en las circunstancias del caso concreto, el cumplimiento de los requisitos preestablecidos y

4 Al examinar el caso concreto de la sentencia *CAJAR vs. Colombia*, la Corte destacó que el conjunto de las medidas de vigilancia «fueron desarrolladas sin requerir autorización y control de una autoridad judicial, la que, además de analizar la proporcionalidad de la medida en el caso concreto, debía decidir acerca del modo, el tiempo, los alcances y los límites que se imponían para salvaguardar los derechos de las personas afectadas». Por lo tanto, la Corte concluyó que «esta falta de intervención judicial resultó incompatible con la Convención Americana, la jurisprudencia interamericana y los estándares internacionales antes detallados (supra párrs. 547, 548, 551 y 553)». Caso Miembros de la Corporación Colectivo de Abogados «José Alvear Restrepo» vs. Colombia, Excepciones Preliminares, Fondo, Reparaciones y Costas, Sentencia de 18 de octubre de 2023, párr. 624.

el juicio de proporcionalidad.

En este sentido, la resolución judicial previa debe:

- estar debidamente motivada, a fin de no ser arbitraria, planteando argumentos racionales que demuestren que se han sopesado todos los requisitos constitucionales, legales y convencionales, incluida la prueba de las tres partes (véanse las secciones anteriores), junto con otros elementos que, según su pertinencia, justifiquen la decisión de autorizar o denegar la medida de vigilancia;
- definir los límites en cuanto a la naturaleza, el alcance y la duración de la medida autorizada, basándose en criterios de necesidad y proporcionalidad.

(ii) Registros detallados

La Corte ha detallado además **controles específicos de registro** para las actividades de inteligencia que deberían inspirar la implementación de procedimientos para la supervisión efectiva de las operaciones de vigilancia de las fuerzas de seguridad en general. Como subrayó la Corte, es necesario establecer mecanismos efectivos de control sobre las acciones de vigilancia para evitar abusos o prácticas arbitrarias por parte de las autoridades.

En particular, la Corte sostuvo que **las autoridades estatales deben formalizar las actividades de inteligencia mediante procesos paso a paso**. Esto significa que:

- Las autoridades deben formalizar, por medio de procesos numerados, las distintas actividades de inteligencia, con el debido registro de todas sus etapas, incluido el historial de registros de acceso a sistemas electrónicos.
- Cuando los organismos traten datos personales, deben garantizar salvaguardias importantes (véase *2.6. Salvaguardias adicionales para el tratamiento de datos personales*), lo que significa, en la medida de lo posible, mantener registros que indiquen:
    - la identificación de los responsables del tratamiento de datos;
    - los propósitos para el tratamiento de la información recopilada, indicando el origen y la categoría de los datos;
    - la base jurídica de las operaciones;
    - los plazos de conservación de los datos;
    - las técnicas utilizadas para su tratamiento.
- Las autoridades también deben registrar las operaciones en registros

cronológicos de acceso, alteración, consulta, eliminación y divulgación de datos personales, así como de las personas que accedieron a ellos.

En consecuencia, **las leyes y reglamentos nacionales** deben estipular dichos procedimientos estructurados de control de las actividades de vigilancia. La Corte destacó que **los organismos deben incluir los procesos numerados en los informes periódicos que envían a los órganos de supervisión** (véase *2.5. Supervisión civil independiente*).

(iii) Sistemas de notificación

La Relatoría Especial para la Libertad de Expresión de la CIDH afirmó que la detección de violaciones de los derechos humanos en el contexto de la vigilancia digital **requiere sistemas de notificación que informen a las personas cuando han sido objeto de vigilancia**. En este sentido, el Relator Especial recomendó a los Estados miembros de la Organización de los Estados Americanos (OEA) que establecieran mecanismos de notificación para las personas sometidas a vigilancia.

La recomendación del Relator Especial se vincula con el principio 8 de los Principios Necesarios y Proporcionados sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones. El principio indica que la notificación debe realizarse con tiempo e información suficientes para permitir a las personas afectadas impugnar la decisión o buscar otros recursos. También establece que el retraso en la notificación solo debe producirse cuando dicha notificación ponga en grave peligro el propósito para el que se autorizó la vigilancia, o cuando exista un riesgo inminente de peligro para la vida humana.

La notificación es una medida crucial para garantizar el derecho a un recurso efectivo en caso de abusos en la vigilancia (véase *4. Recurso y reparación*). En consecuencia, la Corte sostuvo que la necesidad de garantizar el derecho a un recurso efectivo llevó a las normas internacionales a exigir a los Estados que notificaran a las personas afectadas por la vigilancia una vez finalizada esta. Sin notificación, es posible que las personas nunca lleguen a tener conocimiento de procedimientos de recopilación de información arbitrarios o desproporcionados que vulneran sus derechos, lo que plantea obstáculos críticos para la investigación de violaciones de los derechos humanos, la reparación adecuada y la no repetición.

2.5. Supervisión civil independiente

Una pieza fundamental en la arquitectura de las salvaguardias es garantizar una supervisión independiente de la vigilancia digital estatal con facultades robustas y adecuadas. **La vigilancia estatal requiere no solo una rigurosa supervisión interna del organismo que la lleva a cabo, sino también una supervisión externa por**

parte de una institución independiente. Esto debe existir además de las órdenes judiciales previas para las medidas de vigilancia y otros procedimientos de control judicial.

La Corte detalló este requisito para las actividades de inteligencia, subrayando que debe tratarse de una institución civil independiente tanto de los servicios de inteligencia como del poder ejecutivo, que rinda cuentas ante las autoridades legislativas, administrativas o judiciales.

La institución debe contar con los conocimientos técnicos y todas las facultades necesarias para desempeñar sus funciones, lo que incluye el acceso pleno y directo a la información y los datos necesarios para cumplir su misión. Por lo tanto, la institución independiente debe tener la facultad de supervisar:

- el cumplimiento del marco jurídico aplicable a las actividades de los organismos, incluidos los instrumentos de derechos humanos;
- la eficiencia y eficacia de sus actividades, con evaluaciones de rendimiento relacionadas que tengan en cuenta los objetivos legítimos perseguidos;
- la situación financiera y presupuestaria de los organismos, así como la gestión de los fondos;
- los métodos y prácticas administrativas de los organismos.

En este sentido, la Comisión Interamericana recomendó a los Estados que establecieran mecanismos independientes de control y supervisión de la seguridad ciudadana. Asimismo, ha sostenido que los Estados deben fortalecer la capacidad técnica de los parlamentos para evaluar y ejercer el control político sobre las políticas de seguridad pública.

La Relatoría Especial para la Libertad de Expresión de la CIDH destacó que los esfuerzos para establecer una autoridad de supervisión civil independiente deberían incluir la consideración del papel de **los procesos de vulnerabilidades equitativas (VEP)**.

Como explicó el Relator Especial, los VEP son procesos gubernamentales a través de los cuales un Estado decide si divulga las vulnerabilidades de software recién descubiertas a las empresas afectadas para que las corrijan, o si las retiene con fines operativos. La explotación de vulnerabilidades por parte del Estado incluye actividades de aplicación de la ley e investigaciones penales, obtención de información para fines de inteligencia y operaciones cibernéticas ofensivas. El análisis que comprende esta decisión es fundamental, ya que mantener en secreto las vulnerabilidades de software puede permitir su explotación por parte de actores maliciosos o abusos de vigilancia, poniendo en peligro la seguridad

del ecosistema digital en general. El Relator Especial señaló que una supervisión genuina requiere necesariamente la participación de representantes independientes expertos del interés público en los VEP, una función que cumpliría la autoridad civil independiente.

2.6. Salvaguardias adicionales para el tratamiento de datos personales

La Corte sostuvo qu**e los Estados deben adoptar políticas tendientes a prohibir el tratamiento de datos personales[5] , salvo cuando esté fundamentado en la ley o se base en el consentimiento libre e informado de la persona afectada**. En cualquier caso, debe ajustarse a los términos de la Convención Americana, en lo que respecta a los fines legítimos y los mecanismos legales. Las operaciones de tratamiento de datos incluyen la recopilación, el almacenamiento, el análisis y la divulgación de datos, entre otras.

Los Estados también deben adoptar medidas positivas para informar a las personas sobre:

- sus derechos en materia de datos (véase *2.7. Derecho a la autodeterminación informativa*);
- las condiciones legales para el tratamiento de datos personales;
- y cuándo los organismos estatales hayan recopilado, almacenado, tratado o divulgado sus datos personales (véase *2.4.(iii) Sistemas de notificación*).

Además, las garantías de protección de datos exigen a las autoridades que:

- Obtengan únicamente datos **verídicos, pertinentes y necesarios** para el cumplimiento estricto de sus funciones, con arreglo al marco legal aplicable.
- Las autoridades deben ejercer su facultad de tratar datos personales de conformidad con los **fines que justificaron su recopilación**, y únicamente durante **el tiempo imprescindible** para cumplir dichos fines.
- La forma en que las instituciones estatales gestionan la información personal debe garantizar que esta se **mantenga completa, exacta, actualizada y segura**.
- Esto último exige que las autoridades empleen los mecanismos adecuados y

5 El concepto de «datos personales» adoptado por la Corte es «la información que identifica o puede usarse de manera razonable para identificar a una persona física de forma directa o indirecta», lo que incluye los diferentes «factores referidos específicamente de su identidad física, fisiológica, genética, mental, económica, cultural o social [...] expresada de manera numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica, electrónica, visual o de cualquier otro tipo». Caso Miembros de la Corporación Colectivo de Abogados «José Alvear Restrepo» vs. Colombia, Excepciones Preliminares, Fondo, Reparaciones y Costas, Sentencia de 18 de octubre de 2023, párr. 572.

razonables para **prevenir el acceso, la pérdida, la destrucción, la utilización, la modificación o la divulgación no autorizados**.

La Corte señala que el consentimiento libre e informado exige que la persona disponga de información suficiente sobre los datos que se van a recabar, la forma de su obtención, los fines para los que serán utilizados y cualquier posible divulgación, sin dejar lugar a dudas ni ambigüedades sobre la decisión de la persona de dar su consentimiento:

> *«El titular de los datos debería ser capaz de efectuar una elección real y no debería correr ningún riesgo de engaño, intimidación, coacción o consecuencias negativas significativas si se niega a dar el consentimiento».*

Sin embargo, la vigilancia estatal suele llevarse a cabo sin el consentimiento del interesado, dada su naturaleza y sus objetivos. Lo mismo se aplica a las actividades de inteligencia en general.

En consecuencia, **la ley que regula la vigilancia estatal y las actividades de inteligencia**, aprobada por el Congreso y de acceso público, debe estipular específicamente las facultades para recopilar datos personales y crear o mantener bases de datos relacionadas. Según la Corte, esta ley debería regular, de la forma más específica posible:

- los motivos que habilitan la existencia de archivos con datos personales por parte de los organismos de inteligencia, debiendo dichos motivos actuar como una restricción para la labor de las autoridades;
- los tipos y clases de datos personales que las autoridades pueden conservar en sus archivos;
- los parámetros para utilizar, conservar, verificar, rectificar, eliminar o revelar datos personales, en consonancia con las garantías expuestas en los apartados anteriores.

Las autoridades estatales no pueden utilizar sus facultades con fines discriminatorios, incluso en el contexto de la vigilancia digital y las actividades de inteligencia. Como subrayó la Corte, esto significa que no están facultadas para recopilar información, conservar datos o elaborar registros basándose exclusivamente a razones de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier otro tipo, origen nacional o social, posición económica, nacimiento u otra condición social. La Corte añade que, si la consecución de fines legítimos requiere el **tratamiento de datos sensibles,** la ley debe establecer límites sobre los motivos legítimos permitidos, el tipo de datos que las autoridades pueden

recopilar y los criterios adecuados para dicho tratamiento, abarcando únicamente la información que sea estricta y razonablemente necesaria para el cumplimiento del mandato legal de los organismos.

Los organismos de seguridad deben realizar evaluaciones periódicas para determinar si necesitan conservar datos personales en sus archivos y, en caso afirmativo, corroborar su exactitud. Mediante la **depuración de los archivos de inteligencia y seguridad:**

- las autoridades deben eliminar los datos personales que ya no sean necesarios para el cumplimiento de sus funciones;
- las autoridades pueden identificar, clasificar y hacer inventario de los distintos documentos, lo que permite examinar la legalidad de la recopilación y conservación de la información que contienen;
- los organismos mantienen los datos organizados, lo que facilita que los interesados puedan ejercer sus derechos como titulares de datos (véase *2.7. Derecho a la autodeterminación informativa*).

Es importante destacar que la depuración de estos expedientes, es decir, la eliminación de la información personal que ya no es necesaria, no debe obstaculizar el control judicial o la supervisión de las actividades de tratamiento de datos relacionadas en el pasado, ni la capacidad de los interesados para confirmar que dicho tratamiento existió y obtener información sobre los registros pertinentes relacionados.

Además, **la Corte destacó la necesidad de una institución independiente que supervise el tratamiento de datos personales por parte de los organismos de inteligencia**. Dicha institución debe tener acceso a los archivos de inteligencia y estar facultada para ordenar a las autoridades competentes, según cada caso, la eliminación de sus registros, o de la información en estos contenidos, y la revelación de esta información a las personas afectadas. Dependiendo del marco jurídico de los Estados, esta puede ser o no la misma institución de supervisión civil detallada en la sección anterior.

En relación con ello, la Relatoría Especial para la Libertad de Expresión de la CIDH recomendó a los Estados miembros de la OEA que garanticen marcos jurídicos integrales de protección de datos con autoridades de supervisión independientes, aplicables también a los organismos encargados de hacer cumplir la ley y a los de inteligencia, con mandatos específicos para revisar las bases de datos de vigilancia y los sistemas de análisis predictivo a fin de asegurar el cumplimiento de los

estándares de derechos humanos.

2.7. Derecho a la autodeterminación informativa

La Corte hizo hincapié en que es imperativo que se reconozca a las personas **el derecho a acceder y controlar su información personal contenida en los archivos estatales**. Este derecho se deriva de la necesidad de garantizar la autonomía y la autodeterminación de las personas, y abarca las siguientes dimensiones:

- **el derecho a conocer** qué datos se almacenan en los registros o bases de datos estatales, ya sea en soportes físicos, magnéticos, electrónicos o informáticos; el origen de la información; cómo se obtuvo; los fines de su uso; el plazo de conservación; si la institución la comparte con otras entidades o personas y, en caso afirmativo, con qué finalidad; así como las condiciones generales para el tratamiento de sus datos personales;
- **el derecho a reclamar** a la institución que **rectifique, modifique o actualice** su información personal si es inexacta, incompleta o está desactualizada;
- **el derecho a exigir la eliminación, cancelación o supresión**[6] de sus datos en caso de constatar la ilegalidad de su recopilación o conservación, o si no existen razones que justifiquen su permanencia en los archivos o bases de datos estatales, siempre que ello no vulnere otros derechos según un análisis de proporcionalidad y de conformidad con la normativa aplicable;
- **el derecho a oponerse al tratamiento de los datos** si resulta perjudicial para la persona, habida cuenta de su situación particular o de conformidad con la normativa pertinente;
- **el derecho a recibir los datos en un formato estructurado, de uso común y legible por máquina, y el derecho a solicitar la transmisión** de dichos datos sin obstáculos por parte de la autoridad que controla los archivos, siempre que sea posible y de conformidad con las disposiciones legales pertinentes.

6 En cuanto al derecho a la «cancelación» de los datos, la Corte destacó los Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales cuando señalan que: «Este derecho no es absoluto, sino contingente y contextual, y requiere un equilibrio difícil de intereses y principios. El ejercicio del derecho plantea necesariamente cuestiones fundamentales en lo que se refiere no solo a la privacidad, el honor y la dignidad, sino también al derecho de acceso a la verdad, la libertad de información y de expresión, y la proporcionalidad. La legislación nacional de cada Estado debería establecer, en su caso, la existencia del derecho a la cancelación, los requerimientos, plazos, términos y condiciones en los que los titulares podrán ejercer este derecho, así como las causales de improcedencia a su ejercicio». Caso Miembros de la Corporación Colectivo de Abogados «José Alvear Restrepo» vs. Colombia, Excepciones Preliminares, Fondo, Reparaciones y Costas, Sentencia de 18 de octubre de 2023, nota al pie 741.

La Corte consideró que la conjunción de estas garantías constituye un derecho autónomo — **el derecho a la autodeterminación informativa** — reconocido en diversos ordenamientos jurídicos de las Américas y protegido por la Convención Americana. La Corte destacó en particular los artículos 11 (derecho a la vida privada), 13 (derecho de acceso a la información, derivado del contenido del artículo 13(1)) y 25, como una dimensión de la protección judicial.

El derecho a la autodeterminación informativa sirve para garantizar otros derechos, como la privacidad, la protección del honor, la salvaguardia de la reputación y, en general, la dignidad de la persona. La Corte subrayó que este derecho abarca cualquier tipo de datos personales en poder de todo órgano público y es igualmente aplicable a los registros o bases de datos a cargo de particulares. La autodeterminación informativa no es un derecho absoluto y puede ser restringida o limitada, siempre que las restricciones cumplan la prueba de las tres partes, tal y como se detalla a continuación.

La Corte hizo hincapié en que el ejercicio efectivo del derecho a la autodeterminación informativa:

- Exige a los Estados que proporcionen mecanismos o procedimientos adecuados, ágiles y eficaces, disponibles de forma gratuita, para tramitar y resolver las solicitudes de los titulares de datos para acceder y controlar sus datos.
- A través de estos procedimientos, las autoridades controladoras, o las entidades de supervisión y vigilancia, deben responder a las solicitudes dentro de un plazo razonable y predefinido, y bajo la responsabilidad de funcionarios debidamente capacitados.
- El establecimiento de estos mecanismos es una obligación que se deriva del artículo 2 de la Convención Americana. Esta disposición exige a los Estados miembros que promulguen normas y adopten los procedimientos y prácticas necesarios para dar efecto a los derechos consagrados en la Convención.

La Corte también ha recordado el artículo 25(1) de la Convención, relativo a la protección judicial, para **afirmar la obligación de los Estados de prever y poner en práctica un recurso sencillo y rápido capaz de ofrecer una protección efectiva al derecho a la autodeterminación informativa siempre que las solicitudes de los titulares de datos sean denegadas total o parcialmente**.[7] Las autoridades judiciales

7 Al analizar el caso concreto en la sentencia *CAJAR vs. Colombia*, la Corte señaló: «Como consecuencia, en el eventual caso de conocer y resolver acciones de tutela en materia del derecho a la autodeterminación informativa con relación a datos personales contenidos en archivos de inteligencia, las autoridades judiciales internas necesariamente deberán proveer la máxima protección al derecho, para lo cual habrán de atender al contenido de la Convención Americana, la interpretación que de esta ha efectuado la Corte Interamericana a lo largo de su jurisprudencia y, en particular, los estándares recogidos en este Fallo». Caso de los miembros del Colectivo de Abogados «José Alvear Restrepo» c. Colombia, Excepciones preliminares, Fondo, Reparaciones y Costas, Sentencia de 18 de octubre de 2023, párr. 650.

deben poder examinar la información denegada si lo consideran necesario para dictar una resolución. Además, la Corte subrayó la importancia de contar con una institución independiente que supervise el tratamiento de datos personales por parte de los organismos de inteligencia, con facultades que incluyan la divulgación del contenido de los archivos de datos personales a las personas afectadas (véase *2.6. Salvaguardias adicionales para el tratamiento de datos personales*).

(i) Restricciones válidas del derecho a la autodeterminación informativa en el marco de las actividades de vigilancia e inteligencia

Según la Corte, las restricciones válidas al derecho a la autodeterminación informativa en virtud de la Convención Americana deben cumplir los criterios aplicados al derecho de acceso a la información. A continuación se presenta un resumen de estos requisitos.

1º. Principio de legalidad

Cualquier restricción al derecho a la autodeterminación informativa, como la calificación como reservada de una información en poder de las autoridades de inteligencia, **debe estar previamente fijada por ley** (véase *2.1. Marco jurídico claro y preciso*):

- La previsión legal debe ser clara y específica, detallando en la medida de lo posible qué tipo de información o documentos se consideran reservados y el límite temporal que se aplica para la reserva.
- La ley debe determinar claramente que la reserva es excepcional, ya que supone bloquear el derecho de los titulares a acceder y controlar sus datos personales.

El **principio de máxima divulgación** sigue siendo válido en este contexto, derivado de la presunción de que toda la información es accesible, sujeta a un sistema restringido de excepciones. En consecuencia, la ley debe establecer, con especificidad, los motivos para calificar como reservada determinada información, basándose siempre en su contenido específico. En este sentido, cualquier limitación debe responder a un fin legítimo en una sociedad democrática, de conformidad con el artículo 13(2) de la Convención Americana.[8]

En base a lo anterior, **el marco jurídico debe prever mecanismos para la depuración**

8 En cuanto a los parámetros aplicables, véase Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión. El derecho de acceso a la información en el marco jurídico interamericano. Segunda edición, 2011. Disponible en https://www.oas.org/es/cidh/expresion/docs/publicaciones/acceso%20a%20la%20informacion%202012%202da%20edicion.pdf . Véase también Id. Derecho a la información y seguridad nacional, 2020. Disponible en https://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf .

y desclasificación de los archivos de inteligencia y seguridad, permitiendo el acceso público a los documentos y datos cuya reserva no esté justificada, y definiendo periodos fijos de desclasificación automática de la información.

Estos mecanismos deben salvaguardar la confidencialidad de los datos sensibles o de la información que, de conformidad con la normativa aplicable, no pueda divulgarse sin el consentimiento de su titular. En cualquier caso, esta protección no debe obstaculizar el derecho de los titulares a acceder y controlar sus datos personales cuando no exista otro motivo legítimo que justifique la restricción.

2º. Fin legítimo en una sociedad democrática

La Corte subrayó que un Estado no puede impedir el acceso a cualquier información simplemente porque, en general, se considere relacionada con la protección de la seguridad nacional.

> *«[S]ino que es necesario que la ley designe las categorías específicas y estrictas [de la información] que en función de dicho objetivo son alcanzadas por la reserva».*

En consecuencia, **no resulta compatible con los estándares interamericanos** establecer que un documento es reservado por el solo hecho de pertenecer a un organismo de inteligencia y no con base en su contenido.

La Corte identificó algunas condiciones concretas que podrían legitimar restricciones legales al acceso a la información con el fin de proteger la seguridad nacional en el contexto de las actividades de inteligencia. Entre ellas se incluyen, entre otras, la información sobre planes de defensa en curso, medidas específicas para contrarrestar amenazas concretas, siempre que la efectividad de las medidas dependa de su confidencialidad e información sobre asuntos de seguridad nacional proporcionada por un Estado extranjero o un organismo intergubernamental con una indicación expresa de confidencialidad.

Véase más información en el apartado *2.2. Fines legítimos,* más arriba.

3º. Test de proporcionalidad (idoneidad, necesidad y proporcionalidad en sentido estricto)

La decisión de reservar información en bases de datos de inteligencia o seguridad debe cumplir el test de proporcionalidad. A continuación se exponen los parámetros

importantes establecidos por la Corte:

- la reserva (es decir, la denegación de información) debe ser idónea o adecuada para alcanzar el fin legítimo;
- la reserva debe ser necesaria, o sea absolutamente indispensable, para alcanzar ese fin legítimo, lo que significa que ninguna otra medida sería igualmente útil para alcanzar el objetivo y menos gravosa para el derecho de acceso a la información y la autodeterminación informativa;
- la reserva debe ser estrictamente proporcional, de modo que la restricción de estos derechos no sea excesiva en comparación con los beneficios de mantener la confidencialidad de la información para cumplir con el fin perseguido.

La aplicación adecuada del test de proporcionalidad **puede permitir a menudo al menos un acceso parcial** a determinados archivos, documentos o datos.

Véase más información en el apartado *2.3. Idóneo, necesario y proporcionado,* más arriba.

4º. Decisión motivada

Las autoridades competentes deben emitir una decisión bien fundamentada y coherente con las garantías procesales al denegar las solicitudes de acceso y control de la información personal. Esto significa que deben proporcionar una justificación clara y completa de los motivos de la denegación.

5º. Requisitos adicionales

- Las autoridades **no pueden utilizar la reserva de la información en su poder con el interés encubierto** de favorecer o perjudicar a una determinada actividad o una ideología política, o de cualquier otra manera implicar algún tipo de discriminación (véase *2.6. Salvaguardias adicionales para el tratamiento de datos personales*).
- En cualquier caso, **las autoridades tienen la obligación de administrar y tratar la información de forma adecuada y segura, impidiendo cualquier acceso, divulgación, transmisión, alteración o pérdida no autorizados**. Las autoridades deben asegurarse de que los datos personales no se divulguen ni se pongan a disposición de terceros de forma ilegal.
- Las autoridades también deben **realizar revisiones periódicas para garantizar que sigue existiendo justificación para conservar los datos personales en sus archivos, eliminando la información que ya no sea necesaria**. No obstante, el historial de los registros y las operaciones de tratamiento de datos relacionados

con cualquier información personal debería seguir estando a disposición de las autoridades judiciales, de supervisión y de control, incluso después de que la información personal haya sido eliminada. Los interesados también deberían poder obtener información relativa al historial del tratamiento de sus datos personales, incluso una vez finalizado dicho tratamiento y cuando la información personal relacionada ya no esté disponible en los archivos de inteligencia o de seguridad.

- En casos de **violaciones de los derechos humanos**, la reserva de la información por motivos de interés público o seguridad nacional no puede utilizarse para justificar la negativa de las autoridades a facilitar la información solicitada por entidades judiciales o administrativas que lleven a cabo investigaciones o en el marco de procedimientos judiciales.
- Si se está llevando a cabo una investigación sobre un delito punible, la decisión de calificar como secreta la información y, por lo tanto, denegar su entrega, **nunca puede depender exclusivamente de un órgano estatal cuyos miembros sean sospechosos de haber cometido el delito**.
- La reserva de cualquier información **nunca debe ser una medida de duración indefinida**. La reserva y la denegación de acceso pueden permanecer en vigor mientras sea estrictamente necesario para cumplir el fin legítimo previsto, lo que requiere una revisión periódica de la necesidad de mantenerlas.

3. Transparencia y participación

Las actividades relacionadas con la seguridad, incluidas las medidas y operaciones de vigilancia, no constituyen una zona de excepción a los estándares y garantías de transparencia. Por el contrario, su compatibilidad con los derechos fundamentales exige rendición de cuentas, supervisión pública y participación ciudadana en la definición de las políticas relacionadas y los límites aplicables. Como tal, los principios de máxima divulgación, buena fe y la prueba de las tres partes para limitar los derechos se aplican a las entidades de seguridad al igual que vinculan a otros órganos públicos, incluso cuando están en juego fines de seguridad nacional.

El Sistema Interamericano de Derechos Humanos ha elaborado orientaciones fundamentales sobre la transparencia y la participación en el contexto de las actividades de seguridad. A continuación se presentan algunos aspectos destacados.

La Relatoría Especial para la Libertad de Expresión de la CIDH subrayó **que ciertas categorías de información revisten especial importancia pública**, dada su relevancia para el control democrático y el Estado de Derecho.

Se trata de información sobre: violaciones de los derechos humanos y al derecho internacional humanitario, vigilancia estatal y actos de corrupción y/o relacionados con el manejo de los recursos públicos.

En primer lugar, clasificar como reservada o secreta la información sobre graves **violaciones de derechos humanos** es incompatible con la Convención Americana. Por el contrario, el Estado tiene la obligación proactiva de divulgar la información relacionada, llevar a cabo investigaciones y proporcionar reparación a las víctimas.

En cuanto a **la vigilancia estatal**, el Relator Especial subrayó que es esencial que las instituciones estatales garanticen que las personas estén debidamente informadas, como mínimo, sobre:

- el marco jurídico que rige todos los tipos de vigilancia, tanto encubierta como abierta, incluidas las técnicas de vigilancia indirecta, como la generación de perfiles y la minería de datos;
- los fines legítimos de la vigilancia;
- los procedimientos que deben seguir las autoridades para autorizar y revisar el uso de medidas de vigilancia, incluida la selección de objetivos, los procedimientos de tratamiento de datos y el umbral de sospecha requerido para iniciar o continuar las medidas de vigilancia;
- el tipo de datos personales que las autoridades pueden tratar para fines de seguridad (incluida la seguridad nacional), y los criterios que aplican para el uso, la retención, la eliminación y la transferencia de los datos;
- los protocolos para el intercambio, el almacenamiento y la destrucción del material interceptado;
- las entidades autorizadas para llevar a cabo y supervisar acciones de vigilancia;
- las estadísticas sobre las acciones de vigilancia estatal y el uso de herramientas digitales.[9]

En este sentido, el Relator Especial recomendó directamente a los Estados miembros de la OEA que exijan transparencia en la adquisición y el despliegue de sistemas de vigilancia. Además de los puntos anteriores, los informes públicos sobre la vigilancia digital estatal deberían incluir:

9 El Principio 9 de los Principios Necesarios y Proporcionados sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones detalla un conjunto mínimo de información agregada que los Estados deben divulgar. También hace hincapié en que los Estados no deben interferir con los proveedores de servicios en sus esfuerzos por publicar registros de las solicitudes de datos de las autoridades estatales y los procedimientos que siguen al responder a dichas solicitudes. Véase en https://necessaryandproportionate.org/es/principios/ .

- la divulgación de los contratos gubernamentales y el uso de fondos públicos para equipos y servicios relacionados con la vigilancia;
- los registros de los proveedores de vigilancia y la divulgación de información sobre el grupo de contratistas;
- la revelación de las herramientas adquiridas por el Estado y sus especificaciones.

Por último, la seguridad nacional no puede invocarse como motivo legítimo para **resguardar o ocultar**, de forma directa o como efecto indirecto, **presuntas irregularidades o violaciones a la ley, así como el mal funcionamiento de las instituciones públicas, incluso en asuntos relacionados con el gasto presupuestario**. De hecho, el Estado debe divulgar de forma proactiva información que permita al público conocer de manera clara, completa y oportuna cómo las instituciones de seguridad gestionan sus finanzas y las normas aplicables.

Divulgación parcial

El Relator Especial subrayó que, cuando un registro contiene tanto información que entra como información que no entra dentro de las excepciones al principio de máxima divulgación, la restricción de acceso se aplica únicamente a la información específica que debe ser reservada, y no a la totalidad del documento.

Medidas prácticas de rendición de cuentas en actividades relacionadas con la seguridad

La Comisión Interamericana destacó que las autoridades estatales tienen el deber de ser transparentes y coherentes al **informar sobre los criterios utilizados para asignar recursos a las instituciones públicas involucradas en la seguridad ciudadana.** También deben divulgar **indicadores de desempeño**, permitiendo al público evaluar si el gasto público en seguridad ciudadana está logrando los fines legítimos y los objetivos predeterminados. Además, el público debe conocer los sistemas y procedimientos establecidos para revisar las políticas de seguridad cuando los indicadores revelen problemas y fallas.

Esto se relaciona con **el deber de los Estados de producir, organizar y difundir información sobre las políticas de seguridad**, lo cual constituye una obligación positiva dentro de un modelo democrático de seguridad ciudadana. Entre otras medidas relevantes, la Comisión recomendó a los Estados fomentar **observatorios** a nivel nacional y regional para producir, analizar y dar a conocer información calificada sobre la seguridad ciudadana.

La Comisión también instó a los Estados a adoptar medidas efectivas para prevenir la violencia institucional y el uso excesivo de la fuerza por motivos de

origen étnico-racial y patrones de perfilamiento racial. En este sentido, destacó la importancia de contar con **indicadores de políticas de seguridad pública que ayuden a identificar patrones de discriminación institucional y estructural.**[10]

En términos más generales, la Comisión recomendó a los Estados que pusieran en práctica procedimientos para hacer efectiva la rendición de cuentas de todas las autoridades con responsabilidad en la política sobre seguridad pública, mediante **mecanismos de control internos y externos**. Asimismo, ha subrayado que los Estados deben crear las condiciones necesarias para **una participación social significativa** en las cuestiones relacionadas con la seguridad ciudadana.

Medidas adicionales para contrarrestar los abusos de la vigilancia digital

A su vez, la Relatoría Especial para la Libertad de Expresión recomendó a las empresas que establecieran **procesos independientes de auditoría técnica** que permitan a organizaciones de la sociedad civil y a expertos en derechos humanos cualificados examinar las capacidades de la tecnología de vigilancia y los protocolos de implementación para verificar el cumplimiento de las salvaguardias de derechos humanos y las limitaciones contractuales de uso. En la misma línea, el Relator Especial subrayó que la detección de abusos en la vigilancia digital requiere, entre otras cosas, **asistencia técnica para que las organizaciones de la sociedad civil** identifiquen y documenten los abusos.

4. Recurso y reparación de los abusos de vigilancia

Si bien la vigilancia digital estatal en las Américas está plagada de desafíos y deficiencias en la protección de los derechos, los obstáculos para el recurso y la reparación efectivos de los abusos de vigilancia se destacan como la culminación de muchos problemas entrelazados.

La falta de marcos jurídicos claros, completos, necesarios y proporcionados, las garantías jurídicas insuficientes, los débiles mecanismos de control institucional, la escasa transparencia y la nula o escasa rendición de cuentas se combinan para plantear obstáculos cruciales a las personas afectadas a la hora de buscar y obtener reparación. Aunque los retos son más pronunciados para ciertas prácticas de vigilancia, como las que se dan en el contexto de las operaciones de inteligencia, las

10 «La producción y difusión de información por parte de las autoridades públicas debe atender especialmente la situación de aquellos sectores de la población más vulnerables en lo que se relaciona con la prevención de la violencia. Debe alcanzar en forma prioritaria a la situación de las mujeres, la población afrodescendiente e indígena, a las personas migrantes, y a los niños, niñas y adolescentes». CIDH. Informe sobre Seguridad Ciudadana y Derechos Humanos, 2009, párr. 186. Véase también B. Recomendaciones específicas, punto 18. Disponible en https://hchr.org.mx/publicaciones/nforme-sobre-seguridad-ciudadana-y-derechos-humanos-2009/

actividades relacionadas con la seguridad en general requieren un mayor esfuerzo para esclarecer, investigar, sancionar, reparar y adoptar medidas para prevenir la repetición de la vigilancia arbitraria por parte del Estado.

En un informe reciente, el Relator Especial para la Libertad de Expresión de la CIDH destacó:

> *«Quizás la conclusión más alarmante de este informe es la impunidad generalizada en lo que hace a los abusos de vigilancia en toda la región. A pesar de la amplia documentación sobre operaciones de vigilancia ilegales, ningún Estado de las Américas ha logrado enjuiciar a los responsables de los abusos de vigilancia ni ha proporcionado un recurso significativo a las víctimas. Esta falla sistemática de los mecanismos de rendición de cuentas ha creado un entorno permisivo que fomenta la continuación de las violaciones y demuestra tanto a los actores estatales como a los del sector privado que los abusos de vigilancia no tendrán consecuencias».*

De manera similar, la Corte Interamericana destacó en el *caso CAJAR v. Colombia* que **el artículo 25 de la Convención Americana protege a las personas afectadas por actividades de inteligencia arbitrarias en obtener una reparación efectiva, incluida la compensación por daños y perjuicios**. Esta protección también se aplica a los abusos de vigilancia estatal y a las limitaciones desproporcionadas al derecho a la autodeterminación informativa. Dicha protección exige a los Estados proporcionar un recurso judicial sencillo, rápido y efectivo, cuya decisión debe cumplir plenamente con las garantías del artículo 25.

Según el Relator Especial, la actual situación de impunidad de los abusos de vigilancia en la región podría constituir una violación del derecho a un recurso efectivo consagrado en la Convención Americana.

La Oficina del Relator Especial hizo hincapié en que abordar dicha impunidad exige:

- el enjuiciamiento de los responsables, junto con el reconocimiento del daño específico causado a las personas;
- el suministro de información completa a las víctimas sobre el alcance y la duración de la vigilancia;
- la destrucción de los datos obtenidos ilegalmente, y
- garantías de que las autoridades estatales no repetirán estas violaciones.

En este sentido, el Relator Especial recomendó a los Estados miembros de la OEA

- la destrucción de los datos obtenidos ilegalmente, y
- garantías de que las autoridades estatales no repetirán estas violaciones.

En este sentido, el Relator Especial recomendó a los Estados miembros de la OEA que **establezcan mecanismos legales para garantizar recursos efectivos** a las víctimas de abusos de la vigilancia, incluidas disposiciones para abordar los retos probatorios y las lagunas jurisdiccionales en los casos de vigilancia digital.

Además, la Comisión Interamericana recomendó que los Estados **mejoren los procesos de selección y formación de los agentes estatales** que participan en actividades de seguridad (incluidas las fuerzas policiales, el poder judicial y la fiscalía).

Por último, es esencial que los Estados **asignen recursos materiales adecuados para garantizar** mecanismos de control significativos, una supervisión independiente sólida, una supervisión judicial rigurosa y estructuras y procedimientos institucionales capaces de cumplir los requisitos de transparencia y autodeterminación informativa. En conjunto, estos elementos constituyen condiciones indispensables para que el recurso y la reparación efectivos de los abusos de vigilancia sean una realidad concreta y no meros compromisos teóricos sobre el papel.

Conclusión

Esta guía tiene por objeto proporcionar una orientación clara y práctica para abordar un problema de larga data en las Américas: la vigilancia arbitraria por parte del Estado, que ahora se ve cada vez más potenciada por las tecnologías digitales.

No debe normalizarse la situación actual de controles débiles que priorizan alegaciones excesivamente amplias de amenazas a la seguridad nacional y al orden público por encima de la rendición de cuentas de las fuerzas policiales y de inteligencia. Debido a la persistente cultura del secretismo y a los obstáculos sistémicos para garantizar recursos efectivos contra los abusos de vigilancia, cabe esperar resistencia por parte de los Estados de la región a las salvaguardias de esta guía. Sin embargo, superar estos obstáculos es precisamente lo que se necesita para proteger los derechos.

El Sistema Interamericano de Derechos Humanos proporciona a los Estados una base sólida para abordar estos desafíos. Desde la Convención Americana sobre Derechos Humanos hasta sentencias históricas como *CAJAR v. Colombia*, los parámetros jurídicos están bien establecidos.

Los Estados deben implementar marcos jurídicos claros y precisos que:

- definan las facultades y limitaciones de la vigilancia;
- garanticen que todas las medidas de vigilancia persigan objetivos legítimos sin fines discriminatorios;
- sometan la injerencia en la privacidad a un riguroso análisis de necesidad y proporcionalidad;
- exijan autorización judicial previa para las medidas de vigilancia digital;
- mantengan registros detallados de las operaciones de vigilancia;
- establezcan instituciones civiles independientes de supervisión con conocimientos técnicos y facultades robustas de aplicación de la ley;
- garantizar el derecho de las personas a la autodeterminación informativa y a una notificación adecuada de medidas de vigilancia;
- y proporcionar recursos y reparación efectivos a las víctimas de abusos en materia de vigilancia.

No se trata de buenas prácticas opcionales, sino de obligaciones pertinentes en virtud del derecho internacional de los derechos humanos. La Convención Americana, interpretada por la Corte Interamericana, establece que los Estados no pueden invocar la seguridad nacional como justificación general para eludir la transparencia, la rendición de cuentas o el respeto de los derechos fundamentales. Cuando las fuerzas de seguridad se alejan de su objetivo último de proteger a las personas y sus libertades, se convierten en la misma amenaza que se supone que deben combatir.

El coste de la inacción se traduce en una erosión de la democracia, una restricción de la libertad de expresión y una disminución de la confianza entre los Estados y sus ciudadanos. Por el contrario, la aplicación de estas salvaguardias fortalece el Estado de Derecho, refuerza las instituciones democráticas y garantiza que las actividades de seguridad sirvan verdaderamente al interés público. Los Estados que adopten estas recomendaciones no solo cumplirán con sus obligaciones internacionales, sino que también construirán estructuras de seguridad más resilientes y respetuosas con los derechos, capaces de hacer frente a amenazas reales sin sacrificar las libertades que deben proteger.

Como ha advertido la Relatoría Especial para la Libertad de Expresión, la impunidad sistémica que rodea a los abusos de vigilancia en toda la región podría constituir en sí misma una violación del derecho a un recurso efectivo. Los Estados deben actuar con decisión para colmar las lagunas jurídicas, dotar de poderes a los órganos de supervisión, garantizar la independencia judicial y establecer mecanismos de rendición de cuentas significativos. Las orientaciones esbozadas en este informe

ofrecen una hoja de ruta fundamental para hacerlo.

Los Estados que sigan estas orientaciones reafirmarán su compromiso con una visión de la seguridad que proteja tanto a las personas como a sus derechos, reconociendo que estos objetivos no son contradictorios, sino fundamentalmente inseparables.