

SEÑORES Y SEÑORAS JUECES DE LA CORTE CONSTITUCIONAL DEL ECUADOR

Señora Jueza ponente, Alejandra Cárdenas Reyes

Ref. Acción pública de inconstitucionalidad No. 86-25-IN

Se presenta como Amicus Curiae

I. IDENTIFICACIÓN DE QUIEN PRESENTA EL AMICUS Y LA ACCIÓN DE QUE SE TRATA

Juan Diego Castañeda, Catalina Moreno, co-directoras de la Fundación Karisma y Javier Ojeda Escudero, consultor de la Fundación Karisma, comparecemos al amparo de lo dispuesto en el Art. 12 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (en adelante LOGJCC) dentro de la acción pública de inconstitucionalidad No. 86-25-IN y presentamos este escrito de AMICUS CURIAE para que sea tomado en consideración al momento de resolver la causa en referencia.

I. ANTECEDENTES

El 18 de julio de 2025, Verónica Yuquilema Yupangui, en su calidad de presidenta de la Fundación Regional de Asesoría en Derechos Humanos (INREDH); Jonathan Michael Finlay Proaño, gerente general de LALIBRETCH Soluciones Tecnológicas S.A.S.; Billy Rodmann Navarrete Benavidez, director ejecutivo del Comité Permanente por la Defensa de los Derechos Humanos (CDH Guayaquil); y Mónica Diego Vicente, directora ejecutiva de la Corporación Promoción de la Mujer (en conjunto, la “parte accionante”), interpusieron una acción pública de inconstitucionalidad, por el fondo, contra la Ley Orgánica de Inteligencia (la “ley

impugnada” o “Ley de Inteligencia”), publicada en el Cuarto Suplemento del Registro Oficial n.º 57 del 11 de junio de 2025, así como contra el Reglamento General a la Ley de Inteligencia (el “reglamento”, y junto con la ley, las “normas impugnadas”), publicado en el Cuarto Suplemento del Registro Oficial n.º 81 del 15 de julio de 2025.

II. DE LA NATURALEZA DEL AMICUS CURIAE

Fundación Karisma es una organización de la sociedad civil legalmente constituida en Colombia que busca la promoción y protección de los derechos humanos en las políticas relacionadas con tecnología. En cumplimiento de su objeto social, Fundación Karisma ha producido análisis legales y técnicos relacionados con la interacción entre tecnologías digitales, las funciones de investigación penal, inteligencia y policía y la protección de derechos humanos. Así mismo, participa activamente de las discusiones públicas sobre la reforma a la ley de inteligencia en Colombia, sigue y comenta el despliegue de tecnologías en este ámbito y acompaña a otras organizaciones de la sociedad civil en Colombia y en la región que promueven los mismos objetivos.

En la AI se solicitó declarar la inconstitucionalidad por el fondo de varios artículos de la Ley Orgánica de Inteligencia y su normativa conexa, el Reglamento General a la Ley Orgánica de Inteligencia, así como la suspensión provisional de los mismos por representar un riesgo inminente de vulneración a derechos fundamentales. En particular, se impugnan los artículos 4, 5, 13, 14, 22, 32, 41, 42, 43, 47, 48, 50, 51, 52, 53, 55 de la Ley Orgánica de Inteligencia y los artículos 9, 13, 16, 17, 25, 33, 34, 35, 36 y la disposición general primera de su Reglamento General. Estas disposiciones contienen definiciones imprecisas sobre conceptos fundamentales en materia de inteligencia (Art. 5 LOI y Arts. 16 y 17 del Reglamento); habilitan un régimen sin mecanismos adecuados de transparencia, fiscalización, rendición de cuentas y control público sobre la ejecución de los recursos públicos asignados al Sistema Nacional de Inteligencia (Art. 13 LOI y Art. 9 del Reglamento), así como del cumplimiento de sus actividades, objetivos, metas e indicadores (Arts. 14, 55, LOI y Art. 25 del Reglamento); promueven la impunidad al carecer de mecanismos de investigación y sanción de los funcionarios del SIN por responsabilidades en las que pudieran incurrir en el ejercicio de sus atribuciones (Arts. 4, 32, 41 y 53 LOI); facultan el acceso y la recolección de cualquier tipo de información sin orden judicial, mecanismos de protección de datos personales, ni mecanismos de oposición y supervisión autónoma (Arts. 42, 43 47, 48, 50, 51 y 52 LOI y Arts. 16,

33, 34, 35, 36 y disposición general primera del reglamento). Todo ello en contravención de los derechos a la seguridad jurídica (Art. 82 de la Constitución), acceso a la información pública (Art. 18.2 de la Constitución), principios de transparencia, fiscalización y rendición de cuentas (artículos 227, 233, 288, 295, 296 y 297 de la Constitución), protección de datos personales (Art. 66.19 de la Constitución), intimidad (Art. 66.20 de la Constitución), inviolabilidad de la correspondencia (Art. 66.21 de la Constitución), y debido proceso (Art. 76 numerales 1, 2, 4, 7 literal a de la Constitución).

III. ANÁLISIS

De conformidad con lo dispuesto en el artículo 417 de la Constitución de la República del Ecuador, los tratados internacionales ratificados por el Estado forman parte del ordenamiento jurídico interno y, en el caso de los instrumentos internacionales de derechos humanos, se aplican con base en los principios pro ser humano, de no restricción de derechos, de aplicabilidad directa y de cláusula abierta. En ese sentido, el análisis que se expone en este *amicus curiae* se circunscribe exclusivamente a los estándares internacionales que han desarrollado el contenido mínimo que debe reunir una ley de inteligencia para prevenir injerencias arbitrarias o ilegales en la privacidad y la protección de datos personales, lo cual, a su vez, puede tener consecuencias lesivas sobre otros derechos fundamentales.

A nivel internacional, la inteligencia es reconocida como una función esencial y reservada del Estado. Esta naturaleza otorga facultades excepcionales, como el acceso a información privada mediante herramientas tecnológicas, sin requerir el consentimiento previo que sí se exige a otras entidades estatales o privadas.¹ Tal excepcionalidad impone la obligación de que las actividades de inteligencia se encuentren estrictamente delimitadas por una ley formal, clara, precisa y accesible, expedida por el poder legislativo, en la que se definan con suficiente detalle la función de inteligencia, los principios que la rigen, los fines legítimos que persigue, las amenazas que justifican su ejercicio, las prohibiciones aplicables, las autoridades competentes, los procedimientos autorizados, el sistema de rendición

¹ Office of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (Human Rights Council 2022) A/HRC/51/17; *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* [525]; The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, 'Compilation of Good Practices on Legal and Institutional Frameworks and Measures That Ensure Respect for Human Rights by Intelligence Agencies While Countering Terrorism, Including on Their Oversight' (2010) A/HRC/14/46 para 9.

de cuentas y el uso conforme a los derechos humanos de la tecnología empleada.

2

En ese sentido, si tales aspectos se regulan en normativas de menor jerarquía o se establecen sin intervención del poder legislativo, se contraviene el principio de legalidad, pues el carácter de ley formal asegura que su creación, modificación o derogación esté sometida a los procesos democráticos correspondientes. Además, cada uno de estos aspectos debe estar desarrollado con el nivel de detalle suficiente: de lo contrario, la ambigüedad normativa resulta inconstitucional, ya que genera espacios de discrecionalidad que permiten la comisión de arbitrariedades por parte de las autoridades de inteligencia.³

Sobre esta base, el presente amicus procederá a contrastar la Ley Orgánica con los estándares internacionales, a fin de determinar si satisface las exigencias mínimas del principio de legalidad y evita poner en riesgo los derechos humanos.

Función de la inteligencia y sus principios

Los estándares internacionales coinciden en que la inteligencia, por su naturaleza excepcional y reservada, sólo es legítima en un Estado democrático si se concibe como una función orientada a la protección de las personas y no únicamente a la preservación del Estado.⁴ Una concepción centrada exclusivamente en la seguridad estatal, sin un anclaje explícito en los derechos humanos, ha demostrado en contextos comparados derivar en prácticas de vigilancia arbitrarias contra opositores, periodistas o defensores de derechos humanos, generando graves riesgos para la democracia.

La experiencia comparada de Colombia resulta ilustrativa. La Comisión para el Esclarecimiento de la Verdad (CEV) documentó que la inteligencia estatal, al no estar expresamente vinculada a la protección de las comunidades y de los derechos humanos, fue utilizada bajo un enfoque de “enemigo interno”. Este

² Martin Schenin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while counter terrorism., ‘Compilation of Good Practices on Legal and Institutional Frameworks and Measures That Ensure Respect for Human Rights by Intelligence Agencies While Countering Terrorism, Including on Their Oversight’ (2010) A/HRC/14/46 pt Practices 1 to 5; *Caso Miembros de la Corporación Colectivo de Abogados ‘José Alvear Restrepo’ vs Colombia* (Corte Interamericana de Derechos Humanos) a.2.

³ *Caso Miembros de la Corporación Colectivo de Abogados ‘José Alvear Restrepo’ vs. Colombia* (n 2).

⁴ The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 1) para 9; The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, ‘The Role of Intelligence Agencies and Their Oversight in the Fight against Terrorism’ (2009) A/HRC/13/37 para 20; *Caso Miembros de la Corporación Colectivo de Abogados ‘José Alvear Restrepo’ vs Colombia* (n 1) para 525.

paradigma convirtió en blanco de inteligencia y contrainteligencia a líderes sociales, sindicalistas, periodistas y defensores de derechos humanos, generando graves violaciones y debilitando la democracia. La CEV señaló que esta concepción fue posible precisamente porque los marcos normativos privilegiaron una visión de seguridad centrada en la protección del Estado y no en la dignidad y los derechos de las personas. Este antecedente demuestra que la omisión de este anclaje explícito en los derechos humanos de la Ley Orgánica de Inteligencia y su Decreto Reglamentario no es abstracta, sino que conlleva un riesgo concreto de replicar patrones de persecución y arbitrariedad ya condenados en el derecho internacional de los derechos humanos.⁵

La Ley Orgánica de Inteligencia del Ecuador, en su artículo 5,⁶ define la función de la inteligencia en torno a la seguridad integral, pero omite establecer de forma expresa que su ejercicio debe orientarse también a la garantía y respeto de los derechos humanos. Inclusive el Título V de la Ley, relativo a los subsistemas de inteligencia, solo contempla en el subsistema policial la “protección del libre ejercicio de los derechos”, mientras que el resto de subsistemas se vinculan a otras competencias, cuando la obligación de garantizar derechos humanos debería ser transversal a todas las funciones de inteligencia.

Esta omisión resulta significativa porque priva a la Ley de un elemento esencial para legitimar constitucional e internacionalmente la actividad de inteligencia: su sujeción expresa a la protección de los derechos humanos. Sin este anclaje, la función se presenta como un instrumento de seguridad estatal desprovisto de la orientación democrática que exige el derecho internacional, lo que debilita la legalidad de la norma y abre la puerta a interpretaciones expansivas e incompatibles con el Estado constitucional de derechos.

Ahora bien, como la actividad de inteligencia es reservada y recopila, analiza y distribuye información, internacionalmente se han desarrollado principios que rigen las actividades de inteligencia para evitar violaciones arbitrarias a la privacidad y protección de datos. No son reglas estrictas, sino guías que cubran posibles vacíos en las distintas etapas de la gestión de inteligencia. El alcance y relevancia de dichos principios han aumentado debido a los avances tecnológicos que facilitan las tareas de inteligencia, esto implica que los principios se han

⁵ Comisión de la Verdad en Colombia, ‘Hallazgos y Recomendaciones’ (2022) 154, 187 and 190.

⁶ Artículo 5: La actividad consistente en la obtención, sistematización y análisis de la información específica referida a las amenazas, riesgos y conflictos que afecten a la seguridad integral. La información de inteligencia es sustancial para la toma de decisiones en materia de seguridad.

reinterpretado para adaptarse a las capacidades intrusivas de las herramientas tecnológicas actuales.⁷

Dichos principios, aunque están relacionados unos a otros, para su mejor comprensión se dividen en dos, aquellos que sirven como indicadores para medir la correcta limitación al derecho de privacidad, y los que tienen que ver con la protección de datos que implican un correcto manejo de la información recopilada.

1. Principios como indicador para determinar la correcta limitación a la privacidad. Estos surgen directamente del desarrollo internacional al derecho a la privacidad y su afectación en el marco de las actividades de inteligencia:

- **Necesidad, idoneidad y proporcionalidad:** Implican ponderar la aplicación, dentro de la diversidad de operaciones y tecnologías disponibles para el desarrollo de las labores de inteligencia, de aquellas que menos afecten a la población. Su uso debe ser el necesario para evitar un peligro real e inminente (no solo hipotético) para la protección y garantía de los derechos humanos. Por consiguiente, en cada caso debe evaluarse la duración de la medida, su ubicación y si el alcance de su aplicación resulta proporcional en función de su finalidad.⁸

Estos principios han tomado especial relevancia porque los avances tecnológicos han facilitado la intromisión en la privacidad y datos personales de las personas. Existen varios pronunciamientos de diferentes instituciones internacionales que expresan preocupación por el uso indiscriminado por parte de oficinas de inteligencia del hackeo, vigilancia masiva, biométricos, inteligencia artificial, entre otros⁹ Por esto se recomienda que los Estados se abstengan de su uso hasta tanto se pueda asegurar el cumplimiento de los principios de necesidad y proporcionalidad,

⁷ *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 17) pt a.1 to a.5; The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 20) practice 20.

⁸ Grupo de Trabajo sobre la Protección de los Derechos Humanos en la Lucha contra el Terrorismo del Equipo Especial sobre la Ejecución de la Lucha Contra el Terrorismo, 'Guía de Referencia Sobre Los Derechos Humanos Fundamentales: Infraestructura de Seguridad' (2014). Parr. 16.

⁹ General Assembly, 'The Right to Privacy in the Digital Age' (2019) A/RES/73/179. Page 2.

Office of the United Nations High Commissioner for Human Rights (n 1).

Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Fionnuala Ní Aoláin, 'Human Rights Implications of the Development, Use and Transfer of New Technologies in the Context of Counter-Terrorism and Countering and Preventing Violent Extremism.' (2023) A/HRC/52/39.

a través de una correcta capacidad técnica de control, trazabilidad y mecanismos de bloqueo en caso de un ataque externo.¹⁰

2. Principios relacionados a la protección de datos. Surgen directamente de los instrumentos internacionales enfocados en la protección de datos y su función es llenar los vacíos cuando surgen inconvenientes para procesar información, especialmente con el uso de la tecnología. Cómo se refirió, estos principios están relacionados con los de necesidad, idoneidad y proporcionalidad anteriormente desarrollados, sólo se enuncian de forma separada para una mejor comprensión de su origen. Asimismo, estos se garantizan de forma diferenciada para las funciones de inteligencia:¹¹

- **Lealtad y Minimización.** Los datos recogidos, que pueden incluir datos personales o que hagan identificable a una persona, podrán recolectarse y utilizarse exclusivamente dentro de los límites de la finalidad para la que fueron recabados. Asimismo, deben limitarse en todo momento, a lo necesario para la realización de la finalidad establecida.

La regulación internacional define que una persona física identificable es aquella que puede ser reconocida directa o indirectamente mediante identificadores como nombre, número de identificación, datos de localización, identificador en línea o características físicas, fisiológicas, genéticas, mentales, económicas, culturales o sociales.¹²

- **Calidad.** Exige que los datos sean exactos, precisos, completos y actualizados para cada una de las etapas de la gestión de inteligencia, así como necesarios y proporcionales para cumplir los fines de la inteligencia, de lo contrario se debe depurar la información que no sea relevante para ello o notificar a las personas para que dispongan de su información.

¹⁰ United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (2021) A/HRC/48/31. Para. 59.c.

¹¹ Para el contenido de los principios, adicional a las fuentes que se ponen al pie de página en su enunciación, se tomaron en cuenta las siguientes fuentes: Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales 1990 (Resolución 45/95); Ana Brian Nougères, Special Rapporteur on the right to privacy, 'Proposal for the Updating of General Assembly Resolution 45/95 of 14 December 1990, Entitled "Guidelines for the Regulation of Computerized Personal Data Files"' (2024) A/79/173; Estándares de Protección de Datos Personales para los Estados Iberoamericanos 2016; The Special Rapporteur on the right to privacy, Ana Brian Nougères, 'Privacy and Personal Data Protection in Ibero-America: A Step towards Globalization?' (2022) A/HRC/49/55; General Data Protection Regulation 2016.; Los Principios Actualizados de la OEA sobre la Privacidad y la Protección de Datos Personales

¹² General Data Protection Regulation art 4.1.

Para cumplirlo, debe constituirse un registro cronológico al acceso, alteración, consulta, eliminación o divulgación de documentos, insumos y/o productos de inteligencia y contrainteligencia, así como de las personas que accedieron a ellas.

Esta constante supervisión de la información tiene razón de ser porque cierta información es sensible para las personas, y en contextos particulares puede ocasionar un daño diferenciado si fuera usada de forma incorrecta.¹³

- **Acceso o autodeterminación informativa.** Implica que las personas puedan conocer si su información está cumpliendo la finalidad para la que consintió su recolección, a fin de poder objetar su acceso y eliminación en caso de mal uso.¹⁴ Como regla general este principio tiene aplicación absoluta con los entes estatales y privados. Sin embargo, para las oficinas de inteligencia existe un cumplimiento diferenciado al reconocer que, en ciertas circunstancias, el acceso total o parcial a los archivos de inteligencia no es viable porque compromete su función.¹⁵

Las personas de cuyos datos estén en disposición y con reserva de los organismos de inteligencia, podrán disponer de su información por dos razones. Primero, si esta información deja de cumplir con la finalidad por la que fue recopilada.¹⁶ Segundo, si los mecanismos de rendición de cuentas determinan una irregularidad en la gestión de inteligencia que afecte los derechos de las personas. A partir de ello y en ambos supuestos, se notificará a quien haya sido afectado para que disponga de su información.¹⁷ Para que la autodeterminación informativa de las personas afectadas tenga efectividad, el sistema de inteligencia debe tener procedimientos que garanticen la prevención y el acceso expedito a la justicia.

- **Supervisión humana suficiente.** Garantiza que el uso de tecnologías de vigilancia no reemplace el razonamiento humano en la recolección, análisis y difusión de productos de inteligencia. Los estándares internacionales sugieren que la intervención humana debe ser significativa, como revisar los resultados del procesamiento automático o del

¹³ Principios Actualizados sobre la Privacidad y la Protección de Datos Personales 2021. Principio Nueve.

¹⁴ *ibid.* Principio 8.

¹⁵ *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 1) para 601.

¹⁶ *ibid* 608.

¹⁷ *CASE OF ROMAN ZAKHAROV v RUSSIA* [2015] European Court of Human Rights, Grand Chamber Application no. 47143/06 [287]; *Caso Myrna Mack Chang Vs Guatemala Fondo, Reparaciones y Costas* 180 a 182.

perfilamiento,¹⁸ procurando la exactitud de los datos personales para evitar efectos discriminatorios que pongan en riesgo diversos derechos.

Este principio resulta fundamental en un contexto de avances tecnológicos, ya que evita que las decisiones se basen únicamente en el análisis de tecnología de procesamiento automático.¹⁹

- **Flujo transfronterizo de la información.** Implica una cooperación internacional con otros Estados y organismos de inteligencia siempre que cuenten con un nivel equivalente de protección de los derechos humanos y protección de datos.

Esto incluye que los futuros receptores, controladores y procesadores de la información que operen en más de una jurisdicción o que transmitan datos a una jurisdicción distinta de la suya, puedan garantizar la efectiva y debida responsabilidad. Se garantizará que quienes sean receptores de esa información sean respetuosos en materia de derechos humanos y de la protección de datos. Para ello, el estándar internacional sugiere que se deberá establecer claramente y por escrito, cuáles son las normas que rigen el uso de la información compartida y la forma como éstas garantizarán los derechos humanos y la protección de datos, y cómo el organismo de inteligencia remitente se asegurará de que la información que comparte sea pertinente para el mandato del destinatario, se utilizará de conformidad con las condiciones que se impongan en el acuerdo y para fines que no violen los derechos humanos.²⁰

La Ley de Inteligencia en su artículo 5 contempla los principios de clasificación, complementariedad, ética y probidad, exactitud, integralidad, interoperabilidad, legalidad, necesidad de saber, objetividad, oportunidad, pertinencia, priorización, utilidad exclusiva de la información; los cuales no contemplan con exactitud los referidos anteriormente para salvaguardar la privacidad y protección de datos. Aunque resulten oportunos para fortalecer las actividades de inteligencia, los desarrollados internacionalmente no pueden dejar de mencionarse porque resultan el mínimo indispensable en materia de derechos humanos.

En suma, la ausencia de principios sustantivos orientados a la privacidad y a la protección de datos en la Ley Orgánica de Inteligencia no constituye una omisión

¹⁸ European Data Protection Board, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018).

¹⁹ General Data Protection Regulation art 22; European Data Protection Board (n 18).

²⁰ Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Principio 11.

menor, sino una deficiencia estructural frente a las actividades de inteligencia. El artículo 417 de la Constitución obliga a aplicar de manera directa los estándares internacionales en materia de derechos humanos, y estos han establecido que la legalidad de las injerencias en derechos fundamentales, como la privacidad, solo se cumple cuando el marco normativo incorpora principios claros que guíen la planificación, recolección, análisis y difusión de la información. La falta de estos principios en la normativa ecuatoriana abre espacios de discrecionalidad que habilitan un ejercicio de la inteligencia incompatible con el Estado constitucional de derechos, pues se otorgan facultades intrusivas sin los límites materiales exigidos por el derecho internacional de los derechos humanos.

Fines legítimos y amenazas

De acuerdo con los estándares internacionales, la inteligencia busca detectar, prevenir y superar amenazas que atentan contra fines legítimos que hacen operativo a un Estado democrático. Estos fines mínimos incluyen la protección, respeto y garantía de los derechos humanos, la seguridad nacional, el mantenimiento del orden público y la salud pública. Los cuales deben tener una definición con un contenido mínimo de derechos humanos, debido a que así se mitigaría que los fines que busca proteger la inteligencia se usen de forma discrecional y por el contrario guían y legitiman a la institución durante su gestión de inteligencia.²¹ Esto contribuye a crear un verdadero enfoque que considere a la inteligencia como una herramienta para detectar y prevenir violaciones a los derechos humanos o factores de violencia que generan estas violaciones. Ello no excluye que puedan definirse otros fines, siempre que sean coherentes con el objeto y propósito de las obligaciones internacionales del Estado y que cuenten con un contenido mínimo de derechos humanos que evite su uso discrecional.

En particular, el concepto de seguridad nacional ha suscitado preocupación en el ámbito internacional debido a su uso expansivo como justificación de prácticas

²¹ *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 1) pt A.2.1; The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 1) para 9.

abusivas de vigilancia.²² Para mitigar este riesgo, la OACNUDH ha recomendado que su definición incorpore, como mínimo, los siguientes elementos:²³

- a) un enfoque centrado en las personas, vinculado a la democracia, el Estado de derecho y la protección de los derechos humanos;²⁴
- b) la aplicación de un enfoque de seguridad humana, que garantice la dignidad de las personas desde una visión territorial y articulada con entidades internacionales, nacionales y locales, incluidas autoridades indígenas, afrodescendientes y campesinas;²⁵
- c) la distinción de que se trata de una institución civil de inteligencia, Esta distinción permite identificar las causas estructurales que niegan el acceso a derechos desde una perspectiva diferente a la militar, quienes tienen una competencia y visión diferente a la seguridad.²⁶ Esto mitigará cualquier ambigüedad que permita un uso indiscriminado de la inteligencia²⁷; y
- d) la articulación con un sistema de rendición de cuentas, de modo que la seguridad nacional no sea invocada como impedimento para garantizar la supervisión y los derechos de las personas afectadas por la inteligencia y la contrainteligencia.

Finalmente, los estándares internacionales exigen que la ley defina de manera clara cuáles son las amenazas que habilitan el despliegue de la inteligencia. Estas deben estar vinculadas de forma directa a los fines legítimos reconocidos, y fuera de ellas no resulta legal que las autoridades emprendan acciones en este ámbito.

²⁸ Amenazas como el terrorismo, la delincuencia organizada o las economías ilícitas son ejemplos de categorías generalmente aceptadas, pero siempre bajo la condición de que su delimitación sea precisa, taxativa y no quede a la mera

²² The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 1) para 9; *Caso Miembros de la Corporación Colectiva de Abogados 'José Alvear Restrepo' vs Colombia* (n 1) para 532.

²³ 'Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).' (*ONU-DH COLOMBIA*, 4 October 2024) 4

<https://www.hchr.org.co/historias_destacadas/concepto-tecnico-de-onu-derechos-humanos-sobre-la-radicacion-del-proyecto-de-ley-estatutaria-no-225-del-2024-en-el-senado-por-la-cual-se-reforma-la-ley-1621-de-2013-inteligencia-y-contra-inteligencia/> accessed 26 August 2025. Pages 4 and 5.

²⁴ The Special Rapporteur on the right to privacy, Ana Brian Nougères, 'Privacy and Personal Data Protection in Ibero-America: A Step towards Globalization?' (2022) A/HRC/49/55. Par. 5

²⁵ General Assembly, 'Human Security' (2024) A/78/665.

²⁶ *Trueba Arciniega y otros vs México* [2018] Corte Interamericana de Derechos Humanos 369 [21].

²⁷ *Szabó and Vissy v Hungary* [2016] European Court of Human Rights Application no. 37138/14 [73].

²⁸ *Caso Miembros de la Corporación Colectiva de Abogados 'José Alvear Restrepo' vs Colombia* (n 1) para 534.

discrecionalidad administrativa. Inclusive estos conceptos pueden ser amplios para poder ser territorializados a las necesidades de cada Estado.

La Ley Orgánica de Inteligencia del Ecuador, en su artículo 7,²⁹ establece como finalidad la “seguridad integral”, sin precisar qué debe entenderse por seguridad nacional ni desarrollar los fines mínimos exigidos por el derecho internacional. Tampoco incorpora los elementos propuestos por la OACNUDH para asegurar que la seguridad nacional se oriente a la protección de las personas, se fundamente en un enfoque de seguridad humana, se distinga de las funciones militares y se articule con mecanismos de rendición de cuentas. Esta omisión genera un marco normativo ambiguo, que permite la expansión ilimitada de la función de inteligencia en detrimento de los derechos humanos.

En cuanto a las amenazas, la Ley en su artículo 5,³⁰ no las define de manera concreta ni las vincula a parámetros verificables. Por el contrario, delega a la entidad cabeza del sistema de inteligencia la facultad de determinar qué constituye una amenaza a la seguridad integral, lo que otorga un margen de discrecionalidad incompatible con el principio de legalidad. Al no establecer un catálogo mínimo de amenazas, ni vincularlas explícitamente con fines legítimos reconocidos internacionalmente, la Ley abre la puerta a interpretaciones expansivas que pueden habilitar la vigilancia de fenómenos sociales, políticos o económicos bajo la etiqueta de “amenaza”, sin base legal suficiente.

La falta de definiciones claras de fines legítimos y amenazas convierte a la Ley Orgánica de Inteligencia en una norma ambigua e inconvencional. Su omisión de los elementos mínimos recomendados por la OACNUDH sobre seguridad nacional y su remisión a la discrecionalidad administrativa para calificar amenazas vulnera el principio de legalidad, pues impide establecer límites claros y previsibles a la función de inteligencia. En consecuencia, la norma no satisface las obligaciones internacionales asumidas por el Ecuador y permite que la inteligencia se utilice de manera arbitraria, en contravía de su carácter legítimo de protección de los derechos humanos, la democracia y el Estado de derecho.

²⁹ Artículo 7. El Sistema Nacional de Inteligencia tiene como finalidad la protección de los elementos estructurales del Estado; así como los derechos de las personas en todo tiempo y lugar, frente a las vulnerabilidades, amenazas y riesgos de cualquier tipo.

³⁰ Artículo 5: Son los fenómenos, elementos o condiciones de naturaleza antrópica, caracterizada por su capacidad, motivación e intencionalidad de atentar contra los intereses vitales o estratégicos del Estado, las cuales varían constantemente con el apareamiento de nuevos actores y desafíos en los ámbitos políticos, sociales, económicos, ambientales, tecnológicos, criminales y estructurales del Estado.

Sistema de rendición de cuentas

La gestión de la labor de inteligencia debe contar con mecanismos de control y rendición de cuentas adaptados a un sistema reservado, independientes e imparciales, que coadyuven entre ellos para evitar extralimitaciones que puedan derivar en violaciones a los derechos humanos, en particular a la vida privada, u otras que puedan derivar como el ejercicio de la defensa de los derechos humanos, libertad de expresión, de reunión y asociación entre otros.³¹

Estos mecanismos deben contar con facultades y experticia suficientes y tener acceso completo a la información recopilada por los organismos de inteligencia, a fin de contar con elementos necesarios para poder supervisar la necesidad, idoneidad y proporcionalidad de las operaciones y técnicas aplicadas, así como que no generan discriminación.³² A partir de ello, se puede confirmar la continuación, suspensión o terminación de cualquier acción de inteligencia, así como controlar el tratamiento correcto de la información recolectada.³³ En el entendido que la información reservada la ocuparán en el marco de sus procedimientos con la finalidad de confirmar la existencia de una violación de derechos humanos y reparar a las personas afectadas. Cualquier uso de la información fuera de ese marco resultaría en la respectiva responsabilidad.³⁴

La jurisprudencia internacional da mucho margen de discrecionalidad en cómo debe ser un sistema de rendición de cuentas, y sugiere que el estado de derecho se articule para realizar una supervisión política por el congreso y otros órganos más técnicos para supervisar el uso de la información. En todo caso, siempre pide que sea independiente de la injerencia política del ejecutivo o el propio sistema de inteligencia.³⁵

Asimismo, se han definido tiempos para supervisar el correcto tratamiento de la información, datos personas y sensibles recolectados:

³¹ The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 1). Para. 13.

³² Special Rapporteur on the right to privacy, 'Report of the Special Rapporteur on the Right to Privacy' (2017) A/HRC/34/60. Para. 21.

³³ The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 1). Practices 7,8 and 22.

³⁴ *ibid.* Par. 15.

³⁵ Martin Schenin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while counter terrorism. (n 2) para 13.

- a. **El primero relacionado con la autorización del uso de la herramienta.** Su objetivo es supervisar que su empleo es realmente necesario, proporcional e idóneo para lograr proteger una finalidad legítima, así como determinar si no existen medios menos invasivos a los que se pueden recurrir.³⁶

Se ha hecho especial énfasis en el control previo cuando se ocupen las herramientas tecnológicas más invasivas como la recolección masiva de datos y metadatos, así como la vigilancia del ejercicio legítimo de un derecho como la abogacía o el periodismo.³⁷

Asimismo, la jurisprudencia refiere que para no hacer inoperante la actividad de inteligencia, existen excepciones para utilizar herramientas de forma inmediata con la condición de conseguir la referida autorización en un plazo razonable.³⁸

Incluso, para reforzar el respeto a la privacidad con medidas muy invasivas como la recolección masiva de la información se ha recomendado un control durante la recopilación y análisis de la información.³⁹ A partir de dicho escrutinio, la autoridad independiente puede confirmar la continuación, suspensión o terminación de cualquier uso de la tecnología.⁴⁰

- b. **El segundo es un control posterior al uso de la herramienta.** Tiene el objetivo de verificar que la información recolectada es la necesaria, idónea y proporcional a la finalidad a la que fue vinculada en un inicio.

La jurisprudencia internacional refiere que la recolección masiva de información a través de las empresas de telecomunicaciones debe tener un control obligatorio posterior, mientras que otras medidas menos invasivas,

³⁶ *CASE OF BIG BROTHER WATCH AND OTHERS v THE UNITED KINGDOM* [2021] European Court of Human Rights, Grand Chamber Applications nos. 58170/13, 62322/14 and 24960/15; *Centrum för Rättvisa v Sweden* [2021] European Court of Human Rights Application no. 35252/08.

³⁷ *CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM* (n 36); *Pietrzak and Bychawska-Siniarska and Others v Poland* [2024] European Court of Human Rights Apps. nos. 72038/17 & 25237/18; *Centrum för Rättvisa v. Sweden* (n 36).

³⁸ *Pietrzak and Bychawska-Siniarska and Others v. Poland* (n 37).

³⁹ *CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM* (n 36) para 350; Thorsten Wetzling and Kilian Vieth, *Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations* (Heinrich-Böll-Stiftung 2018).

⁴⁰ The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 1). Practice s 7,8 and 22.

por lo menos las autoridades deberían poder supervisar discrecionalmente la información recolectada por la tecnología.⁴¹

En ese sentido, los estándares internacionales subrayan que la supervisión debe abarcar también el tratamiento de los datos personales y sensibles recolectados, lo que incluye la posibilidad de que las personas afectadas activen el principio de autodeterminación informativa. La sentencia CAJAR vs. Colombia de la Corte Interamericana de Derechos Humanos estableció por primera vez en la región la necesidad de mecanismos de rendición de cuentas que permitan a las personas conocer si su información está cumpliendo la finalidad para la que fue recolectada, así como objetar su acceso o exigir su eliminación en caso de uso indebido.⁴²

La jurisprudencia internacional reconoce que, por los objetivos mismos de las actividades de inteligencia, en ciertas circunstancias, el acceso total o parcial a los archivos de inteligencia puede no ser viable. En ese sentido, si una persona acude ante una autoridad de inteligencia, ésta tiene la responsabilidad de brindar los motivos por los cuales no es viable tener acceso a dicha información o, en caso de que los datos ya no cumplan su finalidad para ser almacenada, se garantizará su acceso total o parcial para que la persona afectada determine rectificación y/o eliminación.⁴³

Asimismo, debe existir un órgano independiente con la facultad de revisar la decisión de la autoridad de inteligencia que haya comunicado la existencia o inexistencia de información sobre la persona solicitante. Esta instancia de revisión es clave para asegurar una rendición de cuentas efectiva.⁴⁴

La Ley Orgánica de Inteligencia ecuatoriana regula diversos mecanismos de control y rendición de cuentas:

1. **Informe anual a la Asamblea Nacional** (art. 14). El órgano rector de inteligencia debe rendir cuentas a la Asamblea, pero la Ley no detalla el alcance de este informe ni establece que los legisladores cuenten con asesoría de experticia técnica para evaluar políticamente las actividades de

⁴¹ European Commission for Democracy through Law, 'The Report by the European Commission for Democracy through Law ("Venice Commission") on the Act of 15 January 2016 Amending the Police Act and Certain Other Acts' (2016) Opinion No. 839 / 2016 paras 105 and 106.

⁴² Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Principio 8.

⁴³ *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 1) para 605 y 606; *Pietrzak and Bychawska-Siniarska and Others v. Poland* (n 37) para 248 to 246.

⁴⁴ The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 1). Par. 15.

inteligencia. La ausencia de facultades explícitas de acceso a información reservada debilita el control parlamentario y lo reduce a un ejercicio meramente formal.

2. **Control sobre fondos especiales** (art. 13). El manejo de recursos por parte de la Contraloría se limita a la supervisión financiera, sin facultades para auditar la proporcionalidad o legalidad de las herramientas de vigilancia adquiridas con dichos fondos. Esto genera un vacío respecto de la trazabilidad del uso de recursos en tecnologías invasivas.
3. **Autorización administrativa de medidas intrusivas** (art. 52). Las operaciones de interceptación, retención o apertura de comunicaciones requieren autorización de la máxima autoridad del órgano rector o de los subsistemas. Sin embargo, el órgano rector de ninguna forma cumple con el requisito de independencia.
4. **Mecanismos de control interno** (art. 58). Cada subsistema debe contar con controles internos concurrentes para vigilar fugas, extralimitaciones y afectaciones a derechos. No obstante, la norma no especifica facultades concretas ni garantiza acceso al universo de operaciones. Esto puede impedir que dichos mecanismos supervisen la proporcionalidad de las medidas o el correcto tratamiento de la información, quedando su efectividad a discreción del órgano rector.

El esquema actual de rendición de cuentas en la Ley Orgánica de Inteligencia del Ecuador es insuficiente. Aunque contempla mecanismos de control interno y reportes a la Asamblea, estos no cumplen los requisitos de independencia, experticia técnica ni detalla qué actividades estarán sometidas a una supervisión de extremo a extremo que exige el derecho internacional. La concentración del control en la propia estructura de inteligencia, la ausencia de un órgano externo e independiente y la falta de facultades explícitas para evaluar la necesidad y proporcionalidad de las operaciones, dejan amplios márgenes de discrecionalidad incompatibles con el principio de legalidad.

Asimismo, que las personas no tengan un procedimiento establecido que les permita aplicar el principio de acceso a la información o autodeterminación informativa, hace que el sistema no pueda establecer mecanismos que habiliten los derechos de las personas ni otorga legitimidad a sus actuaciones.

En consecuencia, para ajustarse al artículo 417 de la Constitución y a los tratados internacionales, la Corte debería interpretar que la Ley requiere complementarse con un sistema de supervisión independiente, con acceso pleno a la información reservada, facultades para autorizar previamente las medidas más intrusivas, supervisar su ejecución en tiempo real en casos de vigilancia masiva, y verificar ex post la proporcionalidad del uso y almacenamiento de la información recolectada.

Procedimientos autorizados y formas de recolección de información

Para este amicus, Karisma únicamente se enfocará en los procedimientos previstos en los artículos 47 a 51 relativo a la colaboración con entes públicos o privados, así como el previsto en el artículo 52, de la Ley Orgánica de Inteligencia del Ecuador relativo a la autorización de interceptación de comunicaciones.

El derecho internacional de los derechos humanos, en especial la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) y del Tribunal de Justicia de la Unión Europea (TJUE), ha establecido que toda interferencia con el derecho a la vida privada mediante medidas de vigilancia debe estar sujeta a una supervisión independiente, imparcial y de fin a fin, incluso aquellas relacionadas a solicitar información de usuarios de empresas de telecomunicaciones.

El TJUE, en los casos Digital Rights Ireland, Tele2 Sverige y Watson y La Quadrature du Net, declaró ilegítimos los sistemas de retención general e indiscriminada de datos por parte de empresas privadas, al no limitarse a lo estrictamente necesario ni contar con control independiente previo ni posterior. De igual manera, el TEDH, en Big Brother Watch, Centrum för Rättvisa y Ekimdzhiev v. Bulgaria, subrayó que incluso los metadatos pueden ser tan intrusivos como los contenidos de las comunicaciones, por lo que la supervisión de fin a fin resulta indispensable.

La Ley Orgánica de Inteligencia ecuatoriana prevé en sus artículos 47 a 51 la articulación de los organismos de inteligencia con entidades públicas y privadas, incluidas las de telecomunicaciones, para entregar información o retener datos. Sin embargo, no establece mecanismos claros de supervisión independiente que garanticen que tales medidas sean necesarias y proporcionales. De esta manera, empresas privadas pueden ser compelidas a entregar o conservar datos sin que exista evaluación imparcial sobre la legitimidad o alcance de la medida.

Por su parte, el artículo 52 autoriza la retención, apertura, interceptación o examen de documentos y comunicaciones con la sola autorización de la máxima autoridad

del sistema de inteligencia. Este modelo concentra en el propio aparato de inteligencia tanto la autorización como el control, lo que contradice el estándar internacional de independencia y elimina los contrapesos institucionales necesarios. Al no contar con supervisión previa por un órgano externo ni con revisión posterior obligatoria sobre la proporcionalidad y finalidad de los datos recolectados, el diseño ecuatoriano habilita injerencias arbitrarias.

Los procedimientos autorizados en la Ley Orgánica de Inteligencia del Ecuador son incompatibles con los estándares internacionales de derechos humanos. La concentración del control en la estructura interna de inteligencia y la ausencia de un sistema independiente que supervise la articulación con empresas privadas y las medidas de interceptación vulneran el principio de legalidad y el derecho a la privacidad. Para ajustarse al artículo 417 de la Constitución y a los tratados internacionales, la Corte debe interpretar que estas disposiciones requieren complementarse con un sistema de supervisión externo, imparcial y de fin a fin, con facultades para autorizar previamente las medidas intrusivas, controlar su ejecución en tiempo real en casos de vigilancia masiva y verificar ex post la proporcionalidad y legalidad de la información recolectada.

Tecnología

El derecho internacional reconoce que las labores de inteligencia crecen en alcance rápidamente debido a la creación de nuevas tecnologías;⁴⁵ lo que exige poner las medidas necesarias para que resulten en una herramienta que fortalezca a las instituciones y evitar que éstas violen derechos humanos.⁴⁶ En este apartado se hará un análisis tanto de la adquisición como la utilización de tecnologías.

Adquisición de la tecnología. La adquisición de tecnología para inteligencia implica la intervención de múltiples actores, tanto estatales como privados.⁴⁷ Según los Principios Rectores sobre las Empresas y los Derechos Humanos las empresas son órganos especializados de la sociedad y por ello deben cumplir con las obligaciones de respetar, proteger y cumplir los derechos humanos, así como contribuir en un recurso efectivo en caso de

⁴⁵ *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 1) para 525.

⁴⁶ Office of the United Nations High Commissioner for Human Rights (n 1); General Assembly, 'The Right of Privacy in the Digital Age.' (2020) A/RES/75/176; General Assembly, 'The Right to Privacy in the Digital Age' (n 9).

⁴⁷ Fionnuala Ní Aoláin, 'Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach' para 72.

incumplimiento y contribuir en la reparación.⁴⁸ Por ello, es necesario que estos principios sean tomados en cuenta por las empresas con las que se comercializa.

Por su parte, el Estado tiene la responsabilidad de asegurar que las empresas que operan dentro de su territorio o con las cuales realiza transacciones cumplan con sus obligaciones en materia de derechos humanos. Un ejemplo de esto son los casos Schrems I y Schrems II, sentencias históricas del Tribunal de Justicia de las Comunidades Europeas, que abordan la privacidad y transferencia de datos personales de la Unión Europea a Estados Unidos mediante Facebook. Estas sentencias establecen no solo que las empresas deben ajustarse a parámetros específicos de derechos humanos, sino que subrayan la obligación estatal de proteger los datos personales de sus ciudadanos. Asimismo, ordenan la alineación de las leyes de vigilancia de Estados Unidos con principios de protección de datos, para que el flujo de información entre ambas regiones se mantenga bajo estándares adecuados de derechos humanos.⁴⁹

Ahora bien, para vislumbrar las virtudes o desventajas en materia de derechos humanos que implicaría la adquisición de cierta tecnología, se están utilizando evaluaciones de impacto en la protección de datos. Esta figura es establecida en la normativa internacional de la materia⁵⁰ y actualmente se aplica a tecnologías de procesamiento masivo de la información. La evaluación de impacto describe los posibles riesgos del tratamiento automatizado o la elaboración de perfiles y cómo se puede mitigar. En ese sentido, es viable y razonable hacer una evaluación para la diversidad de herramientas tecnológicas que se puedan adquirir y fortalecer la debida diligencia exigida en los principios de empresas y derechos humanos.

Asimismo, dicha adquisición debe satisfacer como mínimo que la tecnología cuente con capacidades técnicas que permitan evaluar en su uso los principios de necesidad, idoneidad y proporcionalidad, en la medida que limiten su alcance intrusivo. Además, se requiere un registro inmodificable de su uso y mecanismos para detener su operación ante sospechas de abuso, así como de ataques externos.⁵¹

⁴⁸ Principios Rectores sobre las Empresas y los Derechos Humanos 2011.

⁴⁹ European Parliament, 'The CJEU's Schrems Ruling on the Safe Harbour Decision' (2015); European Parliament, 'The CJEU Judgment in the Schrems II Case' (2020).

⁵⁰ General Data Protection Regulation. Recital 91.

⁵¹ *Ní Aoláin* (n 47) para 126.

Utilización. Diferentes sentencias internacionales han analizado el uso de distintas tecnologías que utilizan los cuerpos de inteligencia de los Estados. Entre ellas se incluyen la supervisión de señales transmitidas por vías radioeléctricas o de cables,⁵² líneas de telefonía,⁵³ comunicaciones electrónicas,⁵⁴ así como la capacidad de las referidas instituciones de inteligencia para solicitar la retención masiva de datos y metadatos a las empresas de telecomunicaciones.⁵⁵

En todos estos casos, la jurisprudencia es uniforme en señalar que, al acceder a datos que invaden la privacidad a través de las referidas herramientas tecnológicas, su uso debe estar sujeto a una supervisión independiente, preferiblemente judicial, que garantice el cumplimiento de los principios de necesidad, idoneidad y proporcionalidad para su recolección, almacenamiento y difusión.

Este organismo independiente debe tener poder y capacidad suficiente para acceder a la información reservada de inteligencia, la cual será utilizada exclusivamente dentro del marco de los procedimientos destinados a garantizar la rendición de cuentas.⁵⁶ Cualquier uso de dicha información fuera de ese marco implicaría la correspondiente responsabilidad para la autoridad supervisora.⁵⁷

El artículo 43 de la Ley ecuatoriana autoriza de forma amplia a la entidad rectora, al subsistema militar y al subsistema policial a emplear “técnicas y elementos tecnológicos” en el espectro electromagnético y ciberespacio, sin establecer salvaguardas materiales, evaluaciones de impacto en protección de datos ni procesos de debida diligencia en la contratación de estas tecnologías. Además, declara que el transporte de recursos destinados a estas operaciones es secreto, estratégico y prioritario, prohibiendo cualquier interferencia o inspección, lo que elimina de facto la posibilidad de un escrutinio externo sobre la adquisición y el uso de la tecnología.

⁵² *Centrum för Rättvisa v. Sweden* (n 36).

⁵³ *Haščák v Slovakia* [2022] European Court of Justice App. no. 58359/12, joined with nos. 27787/16 & 67667/16; *Zoltán Varga v Slovakia* [2021] European Court of Justice Apps. nos. 58361/12, 31406/13 & 31283/1.

⁵⁴ *CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM* (n 36).

⁵⁵ *Pietrzak and Bychawska-Siniarska and Others v. Poland* (n 37); *Ekimdzhiev and Others v Bulgaria* [2022] European Court of Justice App. no. 70078/12; *CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM* (n 36); *GD v Commissioner of An Garda Síochána* [2022] European Court of Justice C-140/20; *SpaceNet AG & Telekom Deutschland* [2022] European Court of Justice Joined Cases C-793/19 & C-794/19.

⁵⁶ Special Rapporteur on the right to privacy (n 32). Para. 21.

⁵⁷ The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 1). Par. 15.

Esta habilitación general contrasta con los estándares internacionales que requieren, primero, que la adquisición de tecnología esté sujeta a procesos de debida diligencia, incluyendo evaluaciones de impacto en derechos humanos y protección de datos antes de su compra. La ausencia de estas garantías puede derivar en la adquisición de software o hardware altamente intrusivo (como malware, sistemas de interceptación masiva, biométricos o inteligencia artificial para perfilamiento) sin mecanismos efectivos de mitigación.

Segundo, en cuanto a la utilización, la norma no prevé mecanismos de supervisión externa ni judicial que controlen la proporcionalidad de su uso. Conforme a la jurisprudencia europea (*Big Brother Watch*, *Centrum för Rättvisa*, *Ekimdzhev v. Bulgaria*), el acceso y tratamiento de datos personales mediante tecnologías de vigilancia requiere control independiente en todas las fases del ciclo de inteligencia: desde la autorización previa hasta la eliminación de datos innecesarios. Al no establecer estas salvaguardas, el artículo 43 habilita el despliegue tecnológico sin límites materiales claros y sin garantías de rendición de cuentas.

El marco normativo ecuatoriano en materia de tecnología, previsto en el artículo 43, es incompatible con el artículo 417 de la Constitución y con los estándares internacionales de derechos humanos. Al autorizar de manera amplia el uso de tecnologías en inteligencia y blindar de supervisión sus procesos de adquisición y despliegue, la Ley permite una afectación desproporcionada al derecho a la privacidad y a la protección de datos. Para ajustarse al derecho internacional, la Corte debería interpretar que la Ley debe complementarse con: (i) la obligación de aplicar los Principios Rectores de la ONU sobre Empresas y Derechos Humanos y evaluaciones de impacto en la adquisición de tecnología; y (ii) un sistema de supervisión independiente, imparcial y de fin a fin que autorice previamente, supervise durante la ejecución y controle posteriormente el uso de tecnologías de inteligencia, garantizando que sean necesarias, idóneas y proporcionales a fines legítimos en un Estado democrático.

Personas de especial protección. Artículo 53.

El derecho internacional ha reconocido que las actividades de inteligencia, cuando carecen de límites claros, tienden a dirigirse arbitrariamente contra sectores que cumplen un rol esencial en la democracia. En ese sentido, se han ocupado para

limitar el ejercicio legítimo de derechos como la libertad de expresión, asamblea, defensa de los derechos humanos, abogacía, función jurisdiccional.⁵⁸ Por ello, es necesario que establezca protección reforzada a dichas poblaciones con supervisiones eficientes del tratamiento de su información recolectada.

Estos aspectos se alinean con los estándares internacionales, como los principios 16 y 17 de los Principios Básicos sobre la Función de los Abogados, el artículo 2 de la Declaración sobre Defensores de Derechos Humanos, y las disposiciones sobre libertad de expresión,⁵⁹ y reunión pacífica⁶⁰ y de asociación⁶¹ del Pacto Internacional de Derechos Civiles y Políticos, así como con los principios 1 y 15 de los Principios Básicos sobre la Independencia de la Judicatura.

La Ley Orgánica de Inteligencia contempla en su artículo 53 el principio de no discriminación, lo cual constituye un avance. Sin embargo, la experiencia comparada demuestra que este principio general resulta insuficiente frente al carácter reservado y excepcional de la inteligencia. En la práctica, la ausencia de mecanismos de control específicos deja sin protección a quienes, por la naturaleza de sus actividades, han sido objeto frecuente de vigilancia arbitraria: periodistas, defensores de derechos humanos, líderes sindicales, comunidades indígenas y opositores políticos.

La normativa ecuatoriana no contempla medidas diferenciadas que aseguren, por ejemplo, que cualquier operación de inteligencia que potencialmente afecte a estos grupos esté sujeta a un escrutinio independiente más estricto, con controles previos de necesidad y proporcionalidad, y con procedimientos de verificación posterior sobre el uso de la información recabada. Al no prever estas salvaguardas, la Ley mantiene abiertos márgenes de discrecionalidad que históricamente han derivado en prácticas de persecución política y hostigamiento contra voces críticas, en contravía de los estándares internacionales.

El principio de no discriminación del artículo 53, aunque valioso, no es suficiente por sí solo para garantizar la protección reforzada que requieren los grupos más expuestos al uso arbitrario de la inteligencia. Conforme al artículo 417 de la Constitución, la Corte debería interpretar que la Ley debe complementarse con

⁵⁸ Case of Big Brother Watch and others v The United Kingdom (n 11); Pietrzak and Bychawska-Siniarska and Others v. Poland (n 12); Centrum för Rättvisa v. Sweden (n 9).

⁵⁹ Comité de Derechos Humanos, 'Observación General N° 34 Artículo 19 Libertad de Opinión y Libertad de Expresión' (2011) CCPR/C/GC/34.

⁶⁰ Comité de Derechos Humanos, 'Observación General Núm. 37 (2020), Relativa al Derecho de Reunión Pacífica (Artículo 21)' (2020) CCPR/C/GC/37.

⁶¹ Gina Romero, Special Rapporteur on the rights to freedom of peaceful assembly and of association, 'Protecting the Rights to Freedom of Peaceful Assembly and of Association from Stigmatization' (2024) A/79/263.

mecanismos específicos de supervisión y control reforzado, que aseguren que las operaciones dirigidas o que involucren a periodistas, defensores de derechos humanos, líderes sociales u opositores estén sujetas a controles independientes de fin a fin. Solo así se podrá mitigar el riesgo de vigilancia indebida y dar efectividad al principio de no discriminación, aplicándolo de manera real y práctica en un contexto donde los riesgos de abuso son elevados y comprobados históricamente.

IV. CONCLUSIONES

Del análisis realizado se desprende que la Ley Orgánica de Inteligencia del Ecuador adolece de ambigüedades sustantivas y omisiones regulatorias que la hacen incompatible con el principio de legalidad y con las obligaciones internacionales del Estado en materia de derechos humanos. En particular, la norma no desarrolla con la precisión exigida: (i) la función de inteligencia y los principios que la rigen, incluyendo los relativos a la privacidad y protección de datos; (ii) la determinación clara de los fines legítimos y amenazas que justifican el ejercicio de la inteligencia, quedando abierta a definiciones discrecionales; (iii) un sistema de rendición de cuentas que sea efectivo, con facultades, experticia e independencia suficientes; (iv) la autorización y supervisión de procedimientos altamente intrusivos, al concentrarse en el propio sistema de inteligencia sin control independiente de fin a fin; (v) criterios de debida diligencia para la adquisición y uso de tecnologías de vigilancia; y (vi) salvaguardas reforzadas para sujetos de especial protección, como periodistas, defensores de derechos humanos y líderes sociales.

La ausencia de estos elementos no constituye una omisión menor. Al tratarse de una función excepcional y reservada del Estado, los estándares internacionales han subrayado que la inteligencia solo es legítima y válida en un Estado democrático cuando se orienta a la protección de las personas y está delimitada por salvaguardas legales claras, precisas y accesibles. La actual redacción de la Ley, al permitir amplios márgenes de discrecionalidad, facilita prácticas incompatibles con los derechos a la privacidad, la protección de datos y, por derivación, con el ejercicio de libertades como la de expresión, asociación y defensa de los derechos humanos.

V. PETICIÓN

Conforme lo establece el artículo 12 de la LOGJCC solicitamos:

- V.1. Se acoja el razonamiento jurídico expuesto en el presente amicus curiae.
- V.2. Se nos permita comparecer en la audiencia de sustentación de la causa para exponer a su autoridad los criterios vertidos en el presente amicus curiae.

VI. NOTIFICACIONES

Se recibirán vía correo electrónico en juan.castaneda@karisma.org.co.

FIRMAS



Catalina Moreno Arocha

Co-directora

Fundación Karisma



Juan Diego Castañeda

Co-director

Fundación Karisma



Javier Ojeda Escudero

Consultor

Fundación Karisma