Agosto 29, 2025

Corte Constitucional de Ecuador

Señora Jueza Ponente

Alejandra Cárdenas Reyes

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

Escrito de Amicus Curiae

Reciba un cordial saludo,

Nosotros, Juan Carlos Lara y Jamila Venturini en calidad de co-directores de Derechos Digitales, junto a Paloma Lara Castro y Lucía Camacho Gutiérrez, Directora y Coordinadora de Políticas Públicas de dicha organización respectivamente, comparecemos en ejercicio de lo dispuesto por el Art. 12 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional (en adelante LOGJCC) y presentamos el presente escrito de AMICUS CURIAE dentro de la acción pública de inconstitucionalidad No. 86-25-IN a fin de que sea tomado en consideración al momento de resolver la causa en referencia.

Agradecemos su atención y quedamos a su disposición en caso de que sea oportuno ampliar el detalle de las razones que se expondrán a continuación.

Con deferencia,

Juan Carlos Lara
Co-director ejecutivo
Derechos Digitales · América Latina
jc@derechosdigitales.org

Jamila Venturini
Co-directora ejecutiva
Derechos Digitales · América Latina
jamila@derechosdigitales.org

Paloma Lara Castro
Directora de Políticas Públicas
Derechos Digitales · América Latina
paloma.lara.castro@derechosdigitales.org

Lucia Camacho Gutiérrez
Coordinadora de Políticas Públicas
Derechos Digitales · América Latina
lucia.camacho@derechosdigitales.org

I. SOBRE DERECHOS DIGITALES - LEGITIMACIÓN EN LA CAUSA

Es pertinente indicar que Derechos Digitales[1] es una organización no gubernamental independiente y sin fines de lucro, con sede principal en Santiago de Chile y con alcance latinoamericano. Desde hace 20 años se dedica a la defensa y promoción de los derechos humanos en el entorno digital, con especial énfasis en el impacto que tienen el uso y la regulación de las tecnologías digitales sobre estos derechos.

Fundada en 2005, Derechos Digitales cuenta con una amplia trayectoria en defensa de los derechos humanos frente al impacto sobre ellos en el uso de la tecnología. Ello nos ha llevado a participar en instancias locales, regionales y globales de discusión de políticas públicas, acuerdos y regulaciones que conciernen al despliegue de tecnologías a través de las cuales los Estados ejercitan sus funciones, impactando en el ejercicio de los derechos fundamentales de sus ciudadanas

En el pasado hemos participado, entre otros, en procesos de amparo e inconstitucionalidad en calidad de *amicus curiae* ante la Corte Constitucional de Colombia y Paraguay, y ante el Poder Judicial de la Ciudad de Buenos Aires, en Argentina; así como en procesos de discusión legislativa sobre leyes de inteligencia y lucha contra el terrorismo en países como Brasil, Chile y Colombia,entre otros.

En virtud de lo expuesto, aceptamos muy honorablemente ser tenidos como “amigos de la Corte”, con el propósito de someter a su consideración algunos argumentos para la resolución de la acción de inconstitucionalidad presentada.

II. OBJETO DE ESTE *AMICUS CURIAE*

El objetivo principal de este amicus curiae es acercar respetuosamente a esta Honorable Corte Constitucional un análisis de la Ley Orgánica de Inteligencia (en adelante LOI) aprobada en junio de 2025 y su Reglamento, a partir de los estándares en derechos humanos de alcance interamericano e internacional en materia de privacidad, protección de datos y acceso a la información respecto al abordaje que esos marcos legales hacen de (i) la entrega de bases de datos de actores públicos, privados y personas naturales a la autoridad del Sistema Nacional de Inteligencia (en adelante SNI), (ii) la facultad de interceptación de las telecomunicaciones y de retención de metadatos, (iii) el abordaje de la protección de datos personales en la LOI, y (iv) el acceso a la información pública y la

[1] https://www.derechosdigitales.org/

transparencia sobre el funcionamiento del SNI en su conjunto.

En atención a nuestra experiencia y conocimiento, este *amicus curiae* se centrará en el análisis concreto de los artículos de la Ley Orgánica de Inteligencia[2] y su Reglamento[3] en tanto que son pasibles de generar afectaciones a los derechos a la privacidad y protección de datos, así como la transparencia y acceso a la información. En concreto, abordaremos el contenido de los artículos 13, 14, 47, 48, 50, 51 y la Disposición General Primera de la LOI; así como los artículos 31, 32, 33, 34 y 35 del Reglamento de la LOI.

III. METODOLOGÍA DE ESTE *AMICUS CURIAE*

Para el abordaje de este *amicus curiae*, se delimitará en primer lugar los antecedentes del caso y el contexto de los estándares regionales e internacionales en derechos humanos relevantes para los análisis preliminar y de fondo que serán desarrollados en las secciones subsiguientes. Entre los estándares relevantes, nos referimos a los de privacidad y legalidad, así como los que se han delimitado sobre la vigencia del derecho a la privacidad en el marco de las tareas de inteligencia y contrainteligencia.

En el análisis preliminar, proponemos la visión general que será articulada a lo largo del *amicus curiae;* en el análisis de fondo desarrollamos los argumentos asociados a cinco puntos de interés i) protección de la privacidad en relación con la entrega de datos del sector público, privado y personas naturales al SNI, ii) protección de la privacidad en relación con la interceptación de las comunicaciones y retención de metadatos, iii) la protección de la privacidad en relación con la vigilancia del ciberespacio, iv) el derecho a la protección de datos en las actividades de inteligencia, y por último v)la protección del derecho de acceso a la información pública en el marco de la seguridad nacional.

Al final, elevamos ante esta Honorable Corte las conclusiones y las peticiones asociadas a este escrito.

IV. ANTECEDENTES Y CONTEXTO DEL CASO

En la Acción de Inconstitucionalidad número 86-25-IN a la cual contribuye este *amicus curiae,* los demandantes solicitaron a este Honorable Tribunal declarar la inconstitucionalidad por razones de fondo de varios artículos de la Ley Orgánica de

[2] Publicada en el Registro Oficial Año I – N°57, en Quito, Miércoles 11 de Junio de 2025
[3] Publicado en el Registro Oficial Año I – N°81, en Quito, Martes 15 de Julio de 2025

Inteligencia y su normativa conexa, el Reglamento General a la Ley Orgánica de Inteligencia, así como la suspensión provisional de dichas disposiciones por representar un riesgo inminente de vulneración a derechos fundamentales.

En particular, dicha acción impugna 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 junto con disposición general primera de su Reglamento General. Estas disposiciones presentan serias deficiencias en materia de garantías y control democrático.

Por una parte, la acción señala que dichas disposiciones contienen definiciones imprecisas sobre conceptos fundamentales en materia de inteligencia (Art. 5 LOI y Arts. 16 y 17 del Reglamento). Asimismo, ellas 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).

Del mismo modo, la acción expresa que el contenido de las disposiciones promueve 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). Y en última instancia, ellas facultan el acceso y la recolección de cualquier tipo de información sin orden judicial, carece de mecanismos de protección de datos personales en las actividades de inteligencia, y no cuenta con recursos de oposición a dichas órdenes ni de supervisión autónoma e independiente de su ejecución (Arts. 42, 43, 47, 48, 50, 51 y 52 LOI y Arts. 16, 33, 34, 35, 36 y disposición general primera del reglamento).

Dicha acción de inconstitucionalidad fue admitida en auto 86-25-IN del 5 de agosto de 2025 proferido por este Alto Tribunal, que ordenó entre otros la suspensión provisional de los artículos 5, 13, 22, 41, 42, 43, 47, 48, 50, 51, 52 y 55 de la Ley Orgánica de Inteligencia, así como de los artículos 9, 16, 17, 25, 33, 34, 35, 36 y Disposición General Primera del Reglamento General a la Ley Orgánica de Inteligencia; y que excluyó de la suspensión los artículos 4, 14, 32 y 53 de la Ley y el artículo 13 del reglamento.

Así mismo, en decisión de aclaración del auto admisorio, del 9 de agosto, esta misma Corte reafirmó el contenido de la suspensión de las normas dispuestas originalmente en tanto que se constató “la verosimilitud de la vulneración alegada, la inminencia de su

ocurrencia y la gravedad de sus eventuales efectos, sin que ello suponga un prejuzgamiento sobre la constitucionalidad de la norma".[4]

Por su parte, la acción de inconstitucionalidad en referencia apunta, en términos generales, a la contravención de lo dispuesto en la LOI y el Reglamento, por 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).

IV. 1 Bloque de constitucionalidad y control de convencionalidad

En el marco de este *amicus curiae*, sostenemos que dicha inconstitucionalidad también se fundamenta no solo en la normativa constitucional local, sino en el bloque de constitucionalidad, desarrollado vía jurisprudencial[5] por este mismo Alto Tribunal en tanto que defensora e intérprete de la Carta Fundamental de 2008, y que ha establecido que en él se encuentran integrados el texto de la Convención Americana sobre Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, entre otros instrumentos de derecho regional e internacional.

De la aplicación del bloque de constitucionalidad, esta misma Corte ha afirmado en el pasado que "en cada causa no es suficiente con defender solamente la Constitución, sino también los instrumentos internacionales que la integran".[6] Así como, en materia de jerarquía normativa, ha posicionado a la Declaración Universal de los Derechos Humanos, el Pacto Internacional de los Derechos Civiles y Políticos, y la Convención Americana sobre Derechos Humanos en una posición "normativa superior al resto del ordenamiento".[7]

Además, puntualizamos en la necesidad de someter la normativa demanda por la Acción de Inconstitucionalidad en referencia al control de convencionalidad, en tanto que deber de las autoridades de los Estados parte del sistema interamericano de derechos

[4] Sala de Admisión de la Corte Constitucional, decisión del 9 de agosto, Auto de Aclaración 86-25-IN.
[5] En decisiones como la Resolución 001-2004-DI; la Resolución 002-2005-DI; y la sentencia 0001-009-SIS.
[6] Resolución 001-2004-DI de la Corte Constitucional de Ecuador.
[7] Resolución 0043-07-TC de la Corte Constitucional de Ecuador.

humanos, como es el caso de Ecuador.

En el marco de este *amicus* sugerimos a este honorable tribunal aplicar el control de convencionalidad para el examen de compatibilidad de la Ley Orgánica de Inteligencia y su Reglamento, con la Convención Americana sobre Derechos Humanos, de la cual Ecuador es signataria desde el 22 de noviembre de 1969, habiendo depositado su ratificación el 28 de diciembre de 1977. Así mismo, desde el 13 de Agosto de 1984 el país reconoció la competencia de la Corte Interamericana de Derechos Humanos (en adelante Corte IDH), por lo que el desarrollo jurisprudencial de dicha Corte en interpretación de la CADH y otros instrumentos de alcance interamericano le resultan vinculantes.

El control de convencionalidad, introducido por primera vez por la Corte IDH en el caso Almonacid Arellano y otros *Vs.* Chile, prevé que "los jueces y tribunales internos están sujetos al imperio de la ley y, por ello, están obligados a aplicar las disposiciones vigentes en el ordenamiento jurídico. Pero cuando un Estado ha ratificado un tratado internacional como la Convención Americana, sus jueces como parte del aparato del Estado, también están sometidos a ella, lo que les obliga a velar porque los efectos de las disposiciones de la Convención no se vean mermadas por la aplicación de leyes contrarias a su objeto y fin".[8]

El control de convencionalidad es una institución para la aplicación del derecho internacional de los derechos humanos en el derecho interno que no solo se extiende a la Convención Americana, sino también a sus fuentes y la jurisprudencia de la Corte IDH, así como otros tratados que hacen parte del *corpus iuris* del Derecho Internacional de los Derechos Humanos.[9]

Sobre las decisiones de la Corte IDH, esta misma ha precisado que en tanto que última intérprete de la Convención Americana, su jurisprudencia resulta vinculante a todas las autoridades de los Estados –aun cuando los fallos se refieran a otros Estados parte, la obligatoriedad para todos los Estados miembro de la CADH se deriva del control de convencionalidad mismo–,[10] así como que la interpretación de sus fallos debe sustentarse en los principios y estándares jurisprudenciales sostenidos por la propia Corte IDH.

---

[8] Corte Interamericana de Derechos Humanos, caso Almonacid Arellano y otros vs. Chile. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 26 de septiembre de 2006, párrafo 154

[9] Corte Interamericana de Derechos Humanos, caso Gelman vs. Uruguay, supervisión de cumplimiento de sentencia, resolución de la Corte Interamericana de Derechos Humanos del 20 de marzo de 2013, párrafo 65

[10] Corte Interamericana de Derechos Humanos, caso Comunidad Garífuna de Punta Piedra y sus miembros vs. Honduras. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 8 de octubre de 2015, párrafo 304

En aplicación del control de convencionalidad, las autoridades de los Estados Parte de la CADH, incluidos los jueces y órganos judiciales, deben "prevenir potenciales violaciones a los derechos humanos (...) o bien solucionarlas a nivel interno cuando hayan ocurrido, teniendo en cuenta las interpretaciones de la Corte Interamericana".[11] Entre los efectos que pueden desprenderse del control de convencionalidad sobre una norma o regulación incompatible con la Convención Americana, otros tratados interamericanos, o el Derecho Internacional de los Derechos Humanos, incluyen la supresión o inaplicación general de la norma inconvencional.[12]

En consecuencia, la inaplicación del control de convencionalidad por las autoridades, incluidas las judiciales, "en el marco de sus respectivas competencias y de las regulaciones procesales correspondientes",[13] puede conllevar al incumplimiento del Estado de la obligación de adecuar las disposiciones de derecho interno a la luz de la Convención y otros tratados y obligaciones internacionales en derechos humanos suscritas por éste.[14]

A lo largo de este escrito, identificamos los estándares regionales e internacionales en derechos humanos contravenidos por Ecuador en la regulación de las actividades de inteligencia y contrainteligencia, por lo que solicitamos a este alto Tribunal que en cada ítem declare la inconvencionalidad e inconstitucionalidad de las normas objeto de este análisis.

V. ESTÁNDARES EN DERECHOS HUMANOS RELEVANTES

Sin ánimo exhaustivo, relacionamos algunos de los estándares en derechos humanos del ámbito interamericano e internacional más destacables y relevantes en materia de protección del derecho a la privacidad como derecho articulador de este *amicus*, en especial sobre los requisitos asociados al test tripartito para justificar de manera legítima su limitación, y sobre su vigencia y protección de cara al despliegue de las facultades en materia de inteligencia y contrainteligencia.

---

[11] Corte Interamericana de Derechos Humanos, caso Petro Urrego vs. Colombia. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 8 de julio de 2020, párrafo 107

[12] Corte Interamericana de Derechos Humanos, caso Almonacid Arellano y otros vs. Chile. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 26 de septiembre de 2006, párrafo 121

[13] Corte Interamericana de Derechos Humanos, caso Colindres Schonenberg vs. El Salvador. Fondo, Reparaciones y Costas. Sentencia de 4 de febrero de 2019, párrafo 129

[14] Corte Interamericana de Derechos Humanos, caso Herzog y otros vs. Brasil. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 15 de marzo de 2018, párrafo 292

V. 1 Estándares regionales e internacionales sobre el derecho a la privacidad

El derecho a la privacidad es reconocido en múltiples instrumentos de derechos humanos a nivel regional[15] e internacional[16]. El artículo 11, numeral 2, de la Convención Americana sobre Derechos Humanos (en adelante CADH) prevé que "[n]adie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación" y que "[t]oda persona tiene derecho a la protección de la ley contra esas injerencias o ataques".[17]

En su labor interpretativa de los numerales 2 y 3 del artículo 11 relativos a la protección a la vida privada, la Corte IDH ha precisado su naturaleza y alcance, destacando que:

- El "ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública",[18]

- Abarca "una serie de factores relacionados con la dignidad del individuo, incluyendo, por ejemplo, la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales,[19]

- Aunque las comunicaciones privadas no estén taxativamente reconocidas en el artículo 11 de la CADH, "se trata de una forma de comunicación que, al igual que la correspondencia, se encuentra incluida dentro del ámbito de protección del derecho a la vida privada",[20]

---

[15] Como el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre de 1948 y en los artículos 11 y 13 de la Convención Americana sobre Derechos Humanos ("Pacto de San José") de 1969 (apéndice A) y en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer ("Convención de Belém do Pará") de 1994. También se suman los Principios Interamericanos sobre la Privacidad y la Protección de Datos Personales de 2015, actualizados en 2021.

[16] Como el artículo 12 de la Declaración Universal de los Derechos Humanos; el artículo 17 del Pacto por los Derechos Civiles y Políticos; el artículo 16 de la Convención sobre los Derechos del Niño; artículo 14 de la Convención Internacional sobre la Protección de los Derecho de todos los Trabajadores Migratorios y sus Familiares, entre otros.

[17] Convención Americana Sobre Derechos Humanos, art. 11.2 y art. 11.3

[18] Corte Interamericana de Derechos Humanos, Caso de las Masacres de Ituango vs. Colombia. Sentencia del 1 de julio de 2006, párrafo 193

[19] Corte Interamericana de Derechos Humanos, Caso Artavia Murillo y otros (Fecundación in vitro) vs. Costa Rica. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 28 de noviembre de 2012, párrafo 143

[20] Corte Interamericana de Derechos Humanos, Caso Tristán Donoso vs. Panamá. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 27 de enero de 2009, párrafo 55

- Y que, en ese sentido, el derecho a la vida privada cobija no solo el contenido de las comunicaciones, sino los metadatos asociados a éstas pues "aplica a las conversaciones telefónicas independientemente de su contenido e incluso, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo".[21]

El derecho a la privacidad, protegido tanto en línea como fuera de ella[22], constituye una condición habilitante para el ejercicio de otros derechos, como el de libertad de expresión, protesta pacífica, libertad de asociación, igualdad y no discriminación, entre otros.[23]

El derecho a la vida privada, y por extensión, a la privacidad, "se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos (...) propios del proceso de comunicación".[24]

Ahora bien, su ejercicio no es absoluto: de acuerdo con el artículo 30 de la CADH, puede ser limitado "conforme a las leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas".

Haciendo uso de sus facultades interpretativas, la Corte IDH ha establecido que el derecho a la privacidad puede ser objeto de limitaciones únicamente cuando se satisfacen, de manera estricta los requisitos del estándar tripartito de i) legalidad, ii) fin legítimo y iii) necesidad en una sociedad democrática.[25] De no cumplirse con alguno de estos elementos, toda injerencia al derecho a la privacidad se considera ilegal o arbitraria.

---

[21] Corte Interamericana de Derechos Humanos, Caso Escher y otros vs Brasil. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 6 de julio de 2009, párrafo 114

[22] Consejo de Derechos Humanos, Reporte de la Oficina del Alto Comisionado para los Derechos Humanos, "El Derecho a la Privacidad en la era digital", A/HRC/39/29, del 3 de agosto de 2018, párrafo 11

[23] Consejo de Derechos Humanos, Reporte de la Oficina del Alto Comisionado para los Derechos Humanos, "El Derecho a la Privacidad en la era digital", A/HRC/39/29,del 3 de agosto de 2018, párrafo 11

[24] Corte Interamericana de Derechos Humanos, Caso Escher y otros vs Brasil. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 6 de julio de 2009, párrafo 114

[25]Corte Interamericana de Derechos Humanos, Caso Tristán Donoso vs. Panamá. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 27 de enero de 2009, párrafo 56; Corte Interamericana de Derechos Humanos, Caso Escher y otros vs Brasil. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 6 de julio de 2009, párrafo 116

V. 2 Sobre el principio de legalidad y el derecho a la privacidad

La Opinión Consultiva Nº OC-6/86, relativa a la expresión "leyes" a la que refiere el artículo 30 de la CADH, estableció que dicha noción debe entenderse en sentido formal, es decir, como aquellas normas jurídicas adoptadas "por el órgano legislativo y promulgada[s] por el Poder Ejecutivo, según el procedimiento requerido por el derecho interno de cada Estado".[26] Además, el artículo 30 exige que las leyes que limiten derechos previstos en la CADH persigan un interés general. En la misma Opinión, la Corte IDH precisó que esta expresión está asociada al "bien común" y al "orden público" en un Estado democrático, cuyo fin último y esencial es la "protección de los derechos esenciales de la persona y la creación de circunstancias que le permitan progresar".[27]

La Opinión Consultiva también aborda los escenarios en que una ley delega facultades regulatorias a instrumentos normativos o a autoridades distintas del poder legislativo para limitar derechos. Tal es el caso de las múltiples delegaciones que la LOI otorga a la autoridad del SNI para regular aspectos particularmente sensibles y restrictivos del derecho a la privacidad, como se desarrolla en este *amicus curiae*.

De manera precisa, la Corte IDH ha señalado que tales delegaciones solo resultan válidas si están "autorizadas por la propia Constitución, se ejerzan dentro de los límites impuestos por ella y por la ley delegante, y que el ejercicio de la potestad delegada esté sujeto a controles eficaces, de manera que no desvirtúe, ni pueda utilizarse para desvirtuar, el carácter fundamental de los derechos y libertades protegidos por la Convención".[28]

En este sentido, la reserva de ley se vincula no solo al principio de legalidad, sino también con el de legitimidad, puesto que "sólo la ley adoptada por los órganos democráticamente elegidos y constitucionalmente facultados, ceñida al bien común, puede restringir el goce y ejercicio de los derechos y libertades de la persona humana".[29]

Por otro lado, de conformidad con el Comentario General Nº 16 sobre el Derecho a la Privacidad emitido por el Comité de Derechos Humanos, las injerencias al derecho a la privacidad pueden configurarse bien en ausencia de una ley, o sea, en contravención absoluta del principio de legalidad, por lo que resultan ilegales; o mediante la existencia

[26] Corte Interamericana de Derechos Humanos, Opinión Consultiva OC-6/86 del 9 de mayo de 1986, párrafo 27.
[27] Corte Interamericana de Derechos Humanos, Opinión Consultiva OC-6/86 del 9 de mayo de 1986, párrafo 29.
[28] Corte Interamericana de Derechos Humanos, Opinión Consultiva OC-6/86 del 9 de mayo de 1986, párrafo 36.
[29] Corte Interamericana de Derechos Humanos, Opinión Consultiva OC-6/86 del 9 de mayo de 1986, párrafo 37.

de una ley que en su contenido resulta contraria a los estándares, fines y objetivos fijados por el Pacto de Derechos Civiles y Políticos, por lo que resultan arbitrarias.[30]

De ahí que, no basta que se consagre una ley en sentido formal y material – con el cumplimiento del requisito de que provenga de órganos facultados– que limite el derecho a la privacidad, sino que ésta tiene que responder a un objetivo legítimo, y ser razonable en circunstancias específicas.[31]

V. 3 El principio de legalidad y el derecho a la privacidad aplicado a las actividades de inteligencia

El derecho a la privacidad puede ser restringido en el marco de las actividades estatales de inteligencia y contrainteligencia[32]. En dicho escenario, la Corte IDH ha fijado distintas condiciones que deben ser satisfechas en el ejercicio de dichas facultades estatales, en especial cuando involucra medidas de interceptación de las telecomunicaciones que interfieren con el ejercicio del derecho a la privacidad. Al respecto, ha sostenido que:

- Atendiendo a la propensión al abuso de dicha facultad, las medidas de interceptación deben "basarse en legislación particularmente **precisa, con reglas claras y detalladas**",[33] (énfasis propio).

- Por la naturaleza de la actividad y los medios empleados para la obtención de información, se torna "imprescindible delimitar las **exigencias, requisitos y controles** que se imponen para hacer compatibles aquellas actividades con las condiciones y fines de un Estado de Derecho y, con ello, con el contenido de la Convención Americana",[34] (énfasis propio).

---

[30] CCPR General Comment Nº 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. Adopted at the Thirty-Second Session of the Human Rights Committee, on April 8 1988 (ver párrafo 4).

[31] CCPR General Comment Nº 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. Adopted at the Thirty-Second Session of the Human Rights Committee, on April 8 1988 (ver párrafo 4).

[32] Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la Promoción y la Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha Contra el Terrorismo, Martin Scheinin, A/HRC/13/37, del 28 de diciembre de 2009. Disponible en: https://www.refworld.org/es/ref/infortem/cdhonu/2009/es/72748

[33] Corte Interamericana de Derechos Humanos, Caso Escher y otros vs Brasil. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 6 de julio de 2009, párrafo 118

[34] Corte Interamericana de Derechos Humanos, Caso Miembros de la Corporación José Alvear Restrepo vs Colombia. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 18 de octubre de 2023, párrafo 520

- También, que "[l]as medidas tendientes a controlar las labores de inteligencia **deben ser especialmente rigurosas**, puesto que, dadas las condiciones de reserva bajo las que se realizan esas actividades, pueden derivar hacia la comisión de violaciones de los derechos humanos y de ilícitos penales",[35] (énfasis propio).

- La "vigilancia como la intervención, la grabación y la divulgación de esas comunicaciones quedan prohibidas, salvo en los casos **previstos en la ley y que se adecuen a los propósitos y objetivos de la Convenció**n",[36](énfasis propio).

- Las leyes en este sentido deben definir las actividades de inteligencia, los fines que persiguen y las facultades de los órganos y autoridades competentes. La ley debe "prever, con la **mayor precisión posible**, las distintas amenazas que determinan la necesidad de emprender las actividades de inteligencia por parte de los agentes estatales con competencia en la materia, cuyas facultades también deben **estar clara y exhaustivamente establecidas**, a fin de limitar eficazmente su actuar, impedir la arbitrariedad en su proceder y posibilitar su control y posible deducción de responsabilidades".[37] (énfasis propio).

En resumen, la regulación por vía legal de las actividades de inteligencia debe ser tan concreta, detallada y exhaustiva como sea posible, por los riesgos intrínsecos de afectación de la privacidad asociados a los procesos de recolección de información, que interfieren con dicho derecho y su ámbito de protección.

De igual forma, la Relatoría Especial para la Libertad de Expresión de la CIDH (RELE, en adelante), ha señalado que las normas vagas o ambiguas con facultades amplias y generales son características de los regímenes de vigilancia que conducen a la arbitrariedad y que entrañan una violación al derecho a la privacidad.[38]

También, en el marco de la Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión de 2013, sostuvo junto a sus cosignatarias que la ley que regule el ejercicio de estas facultades "deberá establecer **límites respecto a la**

[35] Corte Interamericana de Derechos Humanos, Caso Myrna Chang vs. Guatemala. Fondo, reparaciones y costas. Sentencia del 25 de noviembre de 2003, párrafo 284

[36] Corte Interamericana de Derechos Humanos, Caso Escher y otros vs Brasil. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 6 de julio de 2009, párrafo 114

[37] Corte Interamericana de Derechos Humanos, Caso Miembros de la Corporación José Alvear Restrepo vs Colombia. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 18 de octubre de 2023, párrafo 528

[38] Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión. Libertad de Expresión e Internet. 31 de diciembre de 2013, CIDH/RELE/INF.11/13, OEA/Ser.L/V/II, párrafo 58

naturaleza, alcance y duración de este tipo de medidas, las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación"[39] (énfasis propio).

En un sentido similar, la Oficina del Alto Comisionado para los Derechos Humanos ha expresado que las limitaciones al derecho a la privacidad deben ser claras, expresas y detalladas en su alcance y objetivos. Y expresó que es el Estado el que tiene la carga argumental de la prueba para explicar la necesidad y razonabilidad de las limitaciones que impone al derecho a la privacidad a través de leyes de inteligencia y contrainteligencia, estableciendo lo siguiente:

> "[T]oda limitación a los derechos a la privacidad [...] debe estar prevista en la ley, y la ley debe ser lo **suficientemente accesible, clara y precisa** para que una persona pueda leerla y saber quién está autorizado a realizar actividades de vigilancia de datos y en qué circunstancias. La limitación debe ser necesaria para alcanzar un objetivo legítimo, así como proporcional al objetivo y la opción menos perturbadora de las disponibles.
>
> "Por otra parte, debe demostrarse que la limitación impuesta al derecho (una injerencia en la vida privada, por ejemplo, con el fin de proteger la seguridad nacional o el derecho a la vida de otras personas) **tiene posibilidades de alcanzar ese objetivo.**
>
> "Es responsabilidad de las autoridades que deseen limitar el derecho demostrar que la limitación está relacionada con un objetivo legítimo. Además, las **limitaciones al derecho a la privacidad no deben vaciar el derecho de su esencia y deben ser compatibles con otras normas de derechos humanos**, incluida la prohibición de la discriminación. Si la limitación no cumple esos criterios, es ilegal y/o la injerencia en el derecho a la privacidad es arbitraria"[40] (énfasis propio).

Por su parte, el entonces Relator Especial sobre la promoción y la protección de los

---

[39] Comisión Interamericana de Derechos Humanos, Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión, Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, "Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión". Disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2

[40] Consejo de Derechos Humanos, Reporte de la Oficina del Alto Comisionado para los Derechos Humanos, "El Derecho a la Privacidad en la era digital", A/HRC/27/37, junio 30, 2014, párrafo 23

derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin, expresó en su informe de 2009 que, tratándose de las facultades de inteligencia, y el despliegue de tecnologías y poderes de vigilancia, se requieren leyes precisas que prevean mecanismos para minimizar y prevenir daños y abusos a los derechos.

En ese sentido, resalta la necesidad de adoptar mecanismos de autorización y revisión judicial independiente, por ejemplo, cuando se trata de la emisión de órdenes de interceptación de las comunicaciones y acceso a metadatos de las personas usuarias de los servicios de telecomunicaciones. Advirtió, además, que en muchos regímenes de inteligencia modernos, estas salvaguardas se han visto reducidas o limitadas, o bien sustituidas por modelos de "autoautorización" secreta.[41]

La ausencia de previsiones detalladas en este sentido en la legislación en cuestión, resulta preocupante desde una perspectiva de derechos humanos, en tanto arroja "dudas sobre si las injerencias son ilegales (y por consiguiente responsables) y necesarias (y por consiguiente proporcionadas").[42] En ese sentido, el Relator Especial ha recomendado que las regulaciones deben fortalecer la supervisión interna como complemento del proceso de autorización independiente y de la supervisión externa. Este sistema integral de supervisión –tanto interna como externa– garantizaría la existencia de recursos efectivos a disposición de las personas, con un acceso significativo a los mecanismos de reparación".[43]

En resumen, en este *amicus* sostenemos que la Ley Orgánica de Inteligencia (LOI) y su Reglamento concentran en el Servicio Nacional de Inteligencia (SNI) un poder informativo sin precedentes en Ecuador y en la región. Estas normas le permiten solicitar de manera indiscriminada información y acceso a bases de datos a entidades públicas y privadas, adquirir tecnologías de vigilancia sin supervisión, interceptar comunicaciones y retener metadatos de forma generalizada por hasta cinco años.

Tales facultades generan riesgos graves de intrusión desproporcionada en la privacidad

[41] Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la Promoción y la Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha Contra el Terrorismo, Martin Scheinin, A/HRC/13/37, del 28 de diciembre de 2009, párrafo 51

[42] Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la Promoción y la Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha Contra el Terrorismo, Martin Scheinin, A/HRC/13/37, del 28 de diciembre de 2009, párrafo 53

[43] Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la Promoción y la Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha Contra el Terrorismo, Martin Scheinin, A/HRC/13/37, del 28 de diciembre de 2009, párrafo 53

de las personas, lo que ha sido advertido por la Corte Interamericana de Derechos Humanos, así como por organismos internacionales como la ONU y la OEA, que insisten en la necesidad de controles estrictos y proporcionales. La privacidad, en este sentido, constituye un derecho esencial que habilita el ejercicio de otros, como la libertad de expresión, la asociación y la protesta pacífica.

En el marco de la CADH, el artículo 11 protege la vida privada, las comunicaciones y la reputación frente a injerencias arbitrarias. La Corte Interamericana ha interpretado que este derecho abarca la dignidad, la identidad y las relaciones personales, e incluye no solo el contenido de las comunicaciones, sino también los metadatos asociados. Aunque el derecho a la privacidad no es absoluto, solo puede limitarse conforme al principio tripartito de legalidad, fin legítimo y necesidad en una sociedad democrática.

El principio de legalidad implica que cualquier restricción debe estar prevista en una ley formal, emanada de órganos democráticamente electos, con un contenido preciso y orientado al bien común. Si bien la ley puede delegar ciertas funciones en órganos de inteligencia, dicha delegación debe estar constitucionalmente autorizada, limitada por la norma que la establece y sometida a controles eficaces. De lo contrario, incluso una ley formal puede resultar arbitraria si contradice los estándares internacionales de protección de los derechos humanos.

En materia de inteligencia, la Corte IDH ha establecido que las facultades de vigilancia y de interceptación de comunicaciones deben estar reguladas con normas claras, detalladas y exhaustivas, que definan los fines, actividades y competencias de los órganos involucrados. Asimismo, se exige un marco de controles estrictos, tanto internos como externos, para prevenir abusos, dado el carácter reservado de estas actividades. Organismos internacionales han subrayado que las normas vagas o ambiguas generan arbitrariedad, por lo que cualquier limitación al derecho a la privacidad debe ser accesible, proporcional, la menos intrusiva posible y siempre justificada por un fin legítimo.

Diversas relatorías de la OEA y la ONU, han recomendado la adopción de mecanismos de autorización judicial independiente para las interceptaciones y el acceso a metadatos, complementados con sistemas de supervisión interna y externa robustos. También destacan la necesidad de recursos efectivos para que los individuos afectados puedan reclamar reparaciones. La ausencia de estas garantías plantearían dudas sobre la

legalidad y proporcionalidad de las medidas legislativas, como las que están previstas en la LOI y su Reglamento.

En conclusión, las facultades amplias y poco delimitadas que estas normas otorgan al SNI ponen en riesgo el derecho a la privacidad en Ecuador, tal y como lo veremos a continuación. Para que sean compatibles con la Convención Americana, se requiere una regulación mucho más detallada, con límites claros, mecanismos de control independientes y garantías de supervisión y reparación efectivas.

VI. ANÁLISIS PRELIMINAR

A lo largo de este *amicus* nos centraremos en sostener que los artículos de la LOI y Reglamento bajo análisis no solo no satisfacen el requisito de legalidad necesario para la regulación y limitación del derecho a la privacidad y protección de datos en el marco de actividades de inteligencia, pues la regulación vigente no es clara, suficiente ni detallada; sino que están elaboradas de manera incompatible con obligaciones internacionales y constitucionales de protección a la privacidad en el marco de las tareas de inteligencia.

Su diseño actual, en cambio, implementa y reactiva lógicas conocidas por la región latinoamericana, basadas en la priorización discursiva de la seguridad nacional como justificación para restringir libertades fundamentales. Esta visión regresiva remite a prácticas propias de los sistemas de inteligencia antidemocráticos de los años 80 y 90, caracterizados por la consolidación de aparatos de vigilancia masiva en la región.

Conforme ha sido sostenido por la Corte Interamericana de Derechos Humanos, sin el cumplimiento del requisito de legalidad, no corresponde avanzar en los análisis subsiguientes sobre la finalidad o necesidad.[44] A lo largo de este escrito de *amicus curia*e sostendremos que los artículos de la LOI y el Reglamento que fueron demandados en acción de inconstitucionalidad N° 86-25-IN no satisfacen el principio de legalidad, y que su contenido es abiertamente incompatible con distintas obligaciones y estándares de derechos humanos a nivel regional e internacional, a los que haremos referencia a lo largo de este escrito.

Al no satisfacerse plenamente el principio de legalidad, se pone en riesgo, entre otros, el

[44] Corte Interamericana de Derechos Humanos, Caso Escher y otros vs Brasil. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 6 de julio de 2009, párrafo 146

principio de seguridad jurídica que debe caracterizar el despliegue de las facultades estatales que puedan resultar invasivas y restrictivas en derechos, como aquellas vinculadas a las actividades de inteligencia y contrainteligencia. Tal como sostienen los accionantes de la demanda de inconstitucionalidad, la ausencia de seguridad jurídica compromete además el equilibrio democrático de poderes, al debilitar las obligaciones estatales de rendición de cuentas, transparencia y sometimiento al escrutinio democrático de la ciudadanía.

VI. 1 Nuestra visión general sobre la LOI y el Reglamento

En el abordaje de este *amicus* mantenemos la tesis según la cual la LOI y el Reglamento centralizan en el Servicio Nacional de Inteligencia (en adelante SNI) un poder informativo sin precedentes en Ecuador y en la región.

Ello, en virtud a que ambos textos habilitan a dicha entidad, rectora del sistema de inteligencia y contrainteligencia del país, a i) formular solicitudes indiscriminadas de información y bases de datos a entidades públicas y privadas, a ii) adquirir, sin mecanismos de supervisión, tecnologías de hardware y software destinadas a desplegar actividades de vigilancia masiva de las comunicaciones en internet, iii) y ejercer facultades abiertas y vagas para la interceptación de las comunicaciones de las personas, así como la retención indiscriminada y generalizada de metadatos por un período excesivo de hasta cinco años lo que constituye una injerencia particularmente invasiva de la privacidad.

Tal y como reconoció en 2009 el entonces Relator Especial Martin Scheinin, en su informe sobre promoción de los derechos humanos en las actividades de inteligencia para la lucha contra el terrorismo, las facultades más críticas de una ley de inteligencia suelen concentrarse en los medios y los mecanismos de producción y recopilación de información y datos. Por su propia naturaleza y condición, esta recopilación suele ser sigilosa, secreta, no advertida ni consentida por su titular, lo que permite al Estado acumular grandes volúmenes de datos personales que, en ausencia de las reglas y salvaguardas adecuadas, pueden derivar en injerencias arbitrarias en la privacidad de las personas.[45]

[45] Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la Promoción y la Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha Contra el Terrorismo, Martin Scheinin, A/HRC/10/3, del 4 de febrero de 2009, párrafos 26 y siguientes

Se trata de una situación particularmente crítica, capaz de generar tensiones entre las actividades de inteligencia y los derechos de las personas. Por ello, la Corte IDH, en el reciente fallo CAJAR *vs* Colombia[46] enfatizó[47] en la necesidad de delimitar con precisión las "exigencias, requisitos y controles" que permitan compatibilizar la recopilación de información, y en especial de datos personales, en el marco de tareas de inteligencia, con las obligaciones establecidas en la Convención Americana sobre Derechos Humanos.

Diversos Organismos universales como regionales, entre ellos el Consejo de Derechos Humanos[48], la Relatoría Especial para la Libertad de Expresión de la ONU y la OEA[49], la Comisión[50] y la Corte Interamericana de Derechos Humanos, han advertido sobre la necesidad de balancear la protección a la seguridad nacional con la salvaguarda de derechos. Asimismo, han reiterado que los poderes de los servicios de inteligencia en materia de vigilancia de las comunicaciones conllevan una alta propensión al abuso, en especial en la era digital, donde el desarrollo tecnológico facilita la recolección intensiva y explotación masiva de información personal de todo tipo.

De ahí la importancia de contar con mecanismos sustanciales y procedimentales de control y supervisión de estas facultades que sean robustos y efectivos, orientados a garantizar la protección de la privacidad. Esta constituye una precondición habilitante para el ejercicio de otros derechos fundamentales como la libertad de expresión, libertad de prensa, derecho a la libre asociación y protesta pacífica, entre otros.

VII. ANÁLISIS DE FONDO

Para profundizar en los elementos antecedentes, abordaremos en las secciones que

[46] El fallo CAJAR vs. Colombia será citado en reiteradas ocasiones en este *amicus curiae*. Aunque su texto es inmediatamente vinculante para Colombia, los principios y estándares fijados por este fallo generan obligaciones para todos los Estados parte de la Convención Americana de Derechos Humanos y que han reconocido la jurisdicción de la Corte IDH. Rescatamos su contenido y destacamos cómo para Ecuador los principios y estándares del fallo le resultan aplicables, por lo que su inobservancia puede ser un factor generador de responsabilidad internacional para el Estado.

[47] Corte Interamericana de Derechos Humanos, Caso Miembros de la Corporación José Alvear Restrepo vs Colombia. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 18 de octubre de 2023, párrafos 520 y 527

[48] Ver informes A/HRC/51/17 de 2022, A/RES/73/179 de 2019, A/HRC/39/29 de 2018, A/HRC/34/L.7/Rev.1 de 2017, A/HRC/27/37 de 2014.

[49] Ver declaraciones conjuntas. En especial, "Declaración conjunta sobre libertad de expresión y elecciones en la era digital de los Relatores Especiales de las Naciones Unidas, OSCE y OEA" 2020; "Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión" n. 2013-2; "Declaración conjunta sobre Wikileaks de los Relatores para la Libertad de Expresión de la CIDH y las Naciones Unidas" n.2010-2.

[50] Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos (Julio, 2020). Derecho a la información y seguridad nacional. OEA/Ser,L/V/II, CIDH/RELE/INF.24/20. Disponible en: https://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf

siguen las disposiciones demandadas en la acción de inconstitucionalidad por temas, de la manera siguiente. En primer lugar, el impacto en el derecho a la privacidad de los artículos 47, 48, 50 y Disposición General Primera; art. 32 y 33 del Reglamento, que tratan en su conjunto sobre la solicitud de datos e información en manos de entidades públicas, privadas y personas naturales En segundo lugar, el impacto en el derecho a la privacidad del artículo 51 de la LOI sobre interceptación de las comunicaciones y acceso a metadatos de las personas usuarias de los servicios de telecomunicaciones. En tercer lugar, el impacto en el derecho a la privacidad del artículo 43 de la LOI sobre vigilancia del espectro electromagnético y el ciberespacio. En cuarto lugar, el abordaje del derecho a la protección de datos personales en el marco de las tareas de inteligencia y contrainteligencia contenido en los artículos 31 y 32 del Reglamento. Y en último lugar, el impacto en el derecho de acceso a la información pública y transparencia de los artículos 13, 14, 43 de la LOI.

Cada sección, encabezada por un resumen, sintetiza los argumentos propuestos ante esta Honorable Corte, y concluye con la petición asociada a la declaratoria de inconvencionalidad e inconstitucionalidad de los artículos impugnados cuando corresponda.

VII. 1 Derecho a la privacidad | Art. 47, 48, 50 y Disposición General Primera; art. 32 y 33 del Reglamento | Sobre la solicitud de información en manos de entidades públicas, privadas y personas naturales

Ni la Ley Orgánica de Inteligencia ni su Reglamento desarrollan con suficiencia ni claridad los requisitos establecidos por los estándares internacionales en materia de protección de datos personales, y de manera específica, por la jurisprudencia de la Corte IDH. En el caso de la decisión del fallo CAJAR vs Colombia, la Corte fijó lineamientos que no son observados, entre ellos: (i) el intercambio de información entre organismos de inteligencia al interior del Estado, sus finalidades precisas y claramente delimitadas, (ii) la descripción clara de las entidades facultadas y autorizadas para entregar o recibir información de inteligencia, y (iii) la consagración de salvaguardas necesarias para la seguridad y protección de la información, en especial para la protección de datos personales potencialmente cubiertos por dicha medida.

La regulación prevista en el marco jurídico de inteligencia vigente ahora mismo en Ecuador no previene la configuración del riesgo de inclusividad excesiva, al que se refiere

el Relator Especial para los derechos humanos en la lucha contra el terrorismo. Conforme será desarrollado, este riesgo se configura cuando las actividades de inteligencia estatal se orientan a la recolección y almacenamiento de grandes volúmenes de información sin un objetivo o motivación claramente definidos.

La regulación de la entrega de datos e información en manos de entidades públicas, privadas y personas naturales incumple el principio de legalidad y, con ello, configura un entramado normativo que limita de manera desproporcionada e irrazonable el derecho a la privacidad en el marco de las tareas de inteligencia. El incumplimiento del principio de legalidad, por la presencia de vacíos normativos reiterados en la LOI y en su Reglamento, resulta en una amenaza para el principio constitucional de seguridad jurídica.

VII. 1. A. Desarrollo de la argumentación

La LOI crea una arquitectura jurídica que subordina a las entidades públicas y privadas al servicio del sistema de inteligencia, facultando al Estado a acumular y utilizar extensas cantidades de datos sin distinción de su tipo o naturaleza, y sin contar con mecanismos adecuados para su protección.

En el articulado, la LOI crea la obligación de entregar la información y bases de datos de manera "oportuna"[51], "completa"[52], "segura"[53], "directa"[54] y "gratuita"[55], así como el deber de mantenerlas actualizadas, vedando a sus responsables la posibilidad de oponerse a dicha entrega, cuestionar o alegar excepciones frente a las solicitudes de la autoridad encargada del Sistema Nacional de Inteligencia (art. 47, 48, 50, y primera disposición general). Incluso cuando se trate de información clasificada en manos de entes públicos, estos se encuentran obligados a cumplir con lo solicitado por el SNI.

En general, la Ley Orgánica de Inteligencia y su Reglamento guardan total silencio sobre las condiciones técnicas y jurídicas que deben regir el intercambio de bases de datos e información entre actores del sistema de inteligencia y otras entidades públicas y privadas. Asimismo, omiten toda referencia a los procesos de intercambio de información entre el sistema de inteligencia ecuatoriano con el de otros países, una práctica habitual de los sistemas de inteligencia modernos. Este vacío normativo, compromete además, la seguridad jurídica que debería de regir en ese tipo de tareas, esenciales en los sistemas

[51] LOI, artículo 47 y artículo 50.
[52] LOI, artículo 50.
[53] LOI, Disposiciones Generales, Primera.
[54] LOI, Disposiciones Generales, Primera.
[55] LOI, Disposiciones Generales, Primera.

de inteligencia.

La deficiente regulación del intercambio de datos e información en la LOI y el Reglamento incrementa lo que se conoce como el riesgo inherente de "inclusividad excesiva". Este fenómeno descrito por Marten Scheinin, Relator Especial de la ONU en asuntos de derechos humanos y Lucha contra el Terrorismo entre 2005 y 2011, alude a la recopilación estatal de información tan solo por su utilidad, sin vinculación con un fin determinado. Tal riesgo se configura a partir del despliegue de un poder extraordinario de centralización de datos e información, que hace de la vigilancia del Estado una práctica cuestionable y problemática.[56]

Sobre este mismo punto, la Corte Interamericana de Derechos Humanos en el fallo CAJAR vs Colombia reiteró[57] la importancia de que (i) el intercambio de información entre organismos de inteligencia al interior del Estado, o entre éste y otros Estados, tengan finalidades precisas y delimitadas en la ley que habilita a dicho intercambio, (ii) que dicha ley describa a las entidades facultadas y autorizadas para entregar o recibir información de inteligencia, y (iii) sean consagradas salvaguardas necesarias para la seguridad y protección de la información, en especial para la protección de datos personales potencialmente cubiertos por dicha medida.

VII. 1. B La entrega de datos e información a cargo de entidades públicas

Esta facultad, de alcance masivo y discrecional, carece de contrapesos en la LOI. La norma exige el cumplimiento del requisito de motivación debida de la medida únicamente cuando la orden de entrega de bases de datos se dirige a entidades del sector público, sin ofrecer justificación alguna para este trato diferenciado respecto de los actores privados (art. 48).

Además, las razones que debe invocar la autoridad responsable del SNI para ordenar dicha entrega se sustentan en fines tan amplios como imprecisos, como la protección de la "seguridad integral del Estado" (art. 48, LOI) sin requisitos adicionales que refuercen la carga argumentativa de la autoridad del SNI.

[56] Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la Promoción y la Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha Contra el Terrorismo, Martin Scheinin, A/HRC/10/3, del 4 de febrero de 2009, párrafo 32 y siguiente

[57] Corte Interamericana de Derechos Humanos, Caso Miembros de la Corporación José Alvear Restrepo vs Colombia. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 18 de octubre de 2023,párrafo 539

De la misma forma, el Reglamento de la Ley Orgánica de Inteligencia[58] omite abordar con suficiencia, detalle y claridad aspectos orgánicos y operativos asociados a la entrega de datos de entidades públicas al Sistema Nacional de Inteligencia y sus respectivos subsistemas. Por ejemplo, el artículo 33 del Reglamento, que se refiere exclusivamente a los requerimientos de información a entidades públicas, prevé que la entidad rectora del SNI podrá solicitar información o datos a cualquier entidad pública pero no describe los criterios que pueden justificar dicha solicitud, ni las condiciones que rigen dicho procedimiento.

El Reglamento no desarrolla ni se refiere al requisito de motivación debida del que trata el artículo 48 de la LOI, por lo que a la fecha no es claro cuándo se debe considerar debidamente motivada una orden de este tipo, cuáles motivaciones y requisitos permitirían satisfacer dicha carga argumental, y cuáles son los escenarios que se desprenden en caso de que dicha orden no esté debidamente motivada.

Por otro lado, el artículo 33 del Reglamento citado omite cualquier previsión sobre la posibilidad de oposición de las entidades públicas requeridas a entregar datos o información, incluso cuando esta se refiera –de manera directa o indirecta– a datos personales vinculados a razones de etnia, género, sexo, lugar de nacimiento, idioma, religión, ideología, opinión política, pertenencia a una organizaciones sindicales, sociales o de derechos humanos.

Se trata de criterios que, en su conjunto, deben ser excluidos de las bases de datos de inteligencia y contrainteligencia, tal y como lo reconoce el artículo 32 del Reglamento que ordena a la Unidad de Protección de Datos verificar que dichos datos no sean almacenados, y el artículo 53 de la LOI que expresamente prohíbe su recolección. Pese a la relevancia de dichos enunciados, ambas normas omiten la creación de mecanismos para asegurar su cumplimiento. Por ejemplo, omiten la creación de una autoridad independiente encargada de la verificación efectiva de su eliminación o borrado en caso

[58] Decreto Nº 52 publicado el 14 de julio de 2025.

hayan sido recolectados o inferidos[59] a partir de la recolección de otros datos personales.

La ausencia de una facultad de oposición aumenta el riesgo de recopilación masiva de información de naturaleza sensible que no debió ser obtenida en primer lugar, pero que las entidades públicas se verán obligadas a entregar sin condición alguna. Se trata de información que, una vez recogida y disponible, aumenta significativamente el riesgo de ser tratada e instrumentalizada en contra de la ciudadanía, ya que se trata de categorías protegidas por el derecho a la protección de datos –en su calidad de "datos sensibles"[60]– como por el derecho a la igualdad, dado el riesgo implícito de discriminación que conlleva.

---

[59] En materia de protección de datos, los datos inferidos –que pueden ser sensibles– son aquellos que se pueden extraer de otros datos que, agregados y en su conjunto, indican características protegidas como las que se enlistan en el artículo 33 del Reglamento. Se trata de datos que no son entregados por su titular, sino creados por el responsable de dichos datos y creados a partir de otro tipo de datos personales en su poder. En su informe, Fundación Vía Libre expresa cómo los datos personales inferidos pueden ser extraídos a partir de herramientas de Big Data, y cómo su protección en ocasiones no es expresa en las leyes de protección de datos personales. Ver: Trovato, M. (2023). Informe. Protección legal de datos personales inferidos. Fundación Vía Libre: Buenos Aires. Disponible en: https://www.vialibre.org.ar/wp-content/uploads/2023/07/ViaLibre2023_Proteccion-legal-datos-personales-inferidos_versionliviana.pdf Por otro lado, autores expertos en los estudios de privacidad y protección de datos como Daniel Solove de hecho indican que por el potencial altamente invasivo de las técnicas y herramientas de inferencia, explotación y tratamiento de los datos personales, en la actualidad deberían considerarse a todos los datos personales como datos sensibles, pues dos datos personales que no sean sensibles pueden indicar o sugerir atributos, características o aspectos sensibles sobre la vida de las personas, convirtiendo en sensibles a datos que en principio las regulaciones no consideran que lo sean. Ver: Solove, Daniel J., Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data (January 21, 2024). 118 *Northwestern University Law Review* 1081 (2024), disponible en: https://ssrn.com/abstract=4322198.

[60] Reconocidos así en distintos instrumentos normativos, como los Principios Interamericanos Actualizados sobre Privacidad y la Protección de Datos Personales según los cuales los datos sensibles son (Principio Nueve): "Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos". También en las Anotaciones a los Principios, se señala que "Según el contexto cultural, social o político, esta categoría podría abarcar, por ejemplo, datos relacionados con la salud personal, las preferencias sexuales o vida sexual, las creencias religiosas, filosóficas o morales, la afiliación sindical, los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona física, las opiniones políticas o el origen racial o étnico, información sobre cuentas bancarias, documentos oficiales, información recopilada de niños y niñas o geolocalización personal. **En ciertas circunstancias podría considerarse que estos datos merecen protección especial porque, si se manejan o divulgan de manera indebida, podrían conducir a graves perjuicios para la persona o a discriminación ilegítima o arbitraria**". Énfasis propio. En: Principios actualizados sobre la privacidad y la protección de datos personales / [Publicación a cargo del Departamento de Derecho Internacional, Secretaría de Asuntos Jurídicos de la Organización de los Estados Americanos] OEA/Ser.D/XIX.20. En: https://www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=1185&lang=2

La ausencia de mecanismos de oposición en manos de entidades públicas se agrava, además, ante la inexistencia de mecanismos efectivos e independientes para supervisar la exclusión efectiva de las piezas de información que estén relacionadas de manera indirecta o indirecta con dichos criterios protegidos, punto que será abordado con mayor profundidad más adelante en esta mismo eje.

Por su parte, el fallo CAJAR vs. Colombia señala que de ser necesario su tratamiento excepcional, se deben delimitar "los motivos para ello, los tipos de datos y los criterios adecuados para su tratamiento, en el entendido que las facultades que se reconozcan a los organismos de inteligencia en este sentido comprenden aquella información estricta y razonablemente necesaria para cumplir sus mandatos".[61] Pero ni la LOI ni el Reglamento prevén con suficiencia ninguno de esos criterios.

Advertimos además cómo el art. 32 del Reglamento omite incluir entre las categorías prohibidas de las bases de datos e información de inteligencia y contrainteligencia la información asociada a niños, niñas y adolescentes (NNA) que, en el fallo CAJAR vs. Colombia, fue identificada como información que debe ser excluida de este tipo de tareas. Esto es especialmente relevante en tanto que emplear información de NNA en tareas de inteligencia entrañaría una violación a los cuatro principios rectores extraídos por la Corte IDH en aplicación de la Convención sobre los Derechos del Niño: (i) principio de no discriminación, (ii) principio del interés superior del niño o niña, (iii) principio del derecho del derecho a la vida, supervivencia y desarrollo, (iv) principio del respeto a su opinión en todo lo que le afecte.[62] Además, se trataría de una injerencia arbitraria e ilegítima del derecho convencional[63] a la privacidad e intimidad "porque en el caso específico de las niñas, niños y adolescentes, su privacidad e intimidad son elementos determinantes para el adecuado desarrollo de su personalidad, puesto que la vida que a futuro emprenderán, en los aspectos intelectual, emocional y otros, se desarrolla desde la infancia y la adolescencia con el auxilio, precisamente, de las condiciones de una vida

[61] Corte Interamericana de Derechos Humanos, Caso Miembros de la Corporación José Alvear Restrepo vs Colombia. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 18 de octubre de 2023, párrafo 579.

[62] Corte Interamericana de Derechos Humanos, Caso Miembros de la Corporación José Alvear Restrepo vs Colombia. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 18 de octubre de 2023,párrafo 631.

[63] La Corte IDH reconoce que los niños, niñas y adolescentes "son titulares de los derechos reconocidos por la Convención Americana [y que] también deben ser protegidos contra todo ataque o restricción indebida a su privacidad e intimidad". Ver: Corte Interamericana de Derechos Humanos, Caso Miembros de la Corporación José Alvear Restrepo vs Colombia, Sentencia del 18 de octubre de 2023. Excepciones preliminares, fondo, reparaciones y costas, párrafo 634.

privada".[64]

Por otro lado, tanto el contenido de la LOI (art. 47, 48 y 50) como el del Reglamento (art. 33) imponen una obligación excesiva de entrega futura y sucesiva de información y su continua actualización[65] –distinta y adicional a la obligación de entrega inicial– a cargo de las entidades públicas requeridas a la entrega de los datos e información, sin que se explique en ninguno de esos dos cuerpos normativos las razones que motivarían dicha medida más allá del empleo repetitivo de la fórmula vaga que alude a "razones de seguridad integral del Estado". De hecho, el artículo 33 numeral 2 del Reglamento señala que más allá de dicha motivación no se puede requerir "otro requisito adicional".

Esta entrega sucesiva y actualizada de información (art. 48, LOI; art. 33 del Reglamento) genera un riesgo intensificado de vigilancia masiva, pues supone la generación continua y en tiempo real de información que facilitaría a la autoridad del SNI, sin limitación ni controles, amasar grandes volúmenes de datos que van más allá de las circunstancias concretas del pedido de entrega inicial, y que por su condición detallada y contextual, supondrían una injerencia desproporcionada e irrazonable en la privacidad de las personas declaradas como objetivo de las tareas de inteligencia y terceras personas vinculadas a estas.

> *VII. 1. C La entrega de datos e información a cargo de entidades privadas y personas naturales*

Tanto la LOI (disposiciones generales, primera) como el Reglamento (art. 35) omiten la delimitación de los criterios operativos y técnicos asociados a la entrega de datos e información a cargo de entidades privadas y personas naturales. Como señalamos anteriormente, las órdenes dirigidas a estos actores no son ni siquiera objeto de motivación debida por parte de la autoridad requirente a cargo del SNI (art. 35 del Reglamento; art. 48 LOI).

---

[64] Corte Interamericana de Derechos Humanos, Caso Miembros de la Corporación José Alvear Restrepo vs Colombia, Sentencia del 18 de octubre de 2023. Excepciones preliminares, fondo, reparaciones y costas, párrafo 634.

[65] Decreto Nº 52 publicado el 14 de Julio de 2025, artículo 33, numeral 2: "Solicitud de entrega y actualización permanente y vigente de las bases de datos e información de la cual dispone cada entidad pública: la máxima autoridad de la entidad rectora del Sistema Nacional de Inteligencia o su delegado podrá solicitar a las entidades públicas, la entrega y actualización permanente y vigente de las bases de datos e información de la cual dispone cada entidad. La solicitud deberá estar motivada por razones de seguridad integral del Estado; la información será entregada, sin otro requisito adicional, de manera impostergable. en el término de dos (2) días contados a partir de la solicitud."

Los únicos artículos del Reglamento[66] y de la LOI[67] que refieren a este tipo de solicitud, señalan que la información requerida debe ser "estrictamente necesaria para el cumplimiento de funciones de inteligencia y contrainteligencia" y disponen que la entidad rectora del SNI regulará posteriormente los requisitos aplicables a este procedimiento. Esta constituye una delegación regulatoria problemática por dos razones.

En primer lugar, porque deja en manos de la propia autoridad requirente de la información la delimitación de un procedimiento que podría diseñarse de forma tal que, o bien sea lo suficientemente laxo que permita justificar sin mayor esfuerzo la solicitud y entrega de datos, o sea tan exigente y detallado su contenido que que legitime la recopilación masiva de información personal, excediendo los límites que deberían regir en un Estado democrático.

En segundo lugar, esta dilación en el diseño del procedimiento de entrega de datos e información genera una incertidumbre normativa respecto de todas las órdenes de entrega de datos e información dirigidas a actores del sector privado, personas naturales y sector público desde la la fecha de expedición del Reglamento, fechado el 14 de julio, hasta que la regulación a cargo de la máxima autoridad del SNI sea finalmente expedida.

Por tanto, solicitamos de manera respetuosa a esta alta Corte que declare la inconvencionalidad de los artículos 47, 48, 50 y la Disposición General Primera de la LOI, y 32, 33, y 35 del Reglamento, en tanto que su vaguedad, imprecisión normativa, y apertura enunciativa atentan contra el principio de legalidad, y habilitan a injerencias arbitrarias sobre el derecho a la privacidad del que son titulares las personas cuyos datos reposan en bases de datos en manos de entidades públicas, privadas y otras personas naturales.

VII. 2 Derecho a la privacidad / Art. 51 de la LOI sobre interceptación de las comunicaciones y acceso a metadatos

La Ley Orgánica de Inteligencia (LOI) regula la interceptación de las comunicaciones sin

[66] Decreto Nº 52 publicado el 14 de Julio de 2025, artículo 35: "Artículo 35.- Requerimientos de información general.- El requerimiento de información a personas naturales o jurídicas, públicas o privadas, podrá efectuarse únicamente cuando la información solicitada sea estrictamente necesaria para el cumplimiento de funciones de inteligencia y contrainteligencia relacionadas con la seguridad integral del Estado. Dicho requerimiento será formulado por la máxima autoridad de la entidad rectora del Sistema Nacional de Inteligencia o por la máxima autoridad del subsistema de inteligencia militar o policial, de conformidad con la normativa secundaria que emita la entidad rectora del Sistema Nacional de Inteligencia y que regule este procedimiento, garantizando el respeto al ordenamiento jurídico vigente y a los derechos y garantías constitucionales de las personas".

[67] LOI, Disposiciones Generales, Primera.

que existan salvaguardas claras para proteger la privacidad de las personas ni mecanismos de control judicial o de justificación rigurosa de las órdenes de interceptación y de retención de los metadatos de las personas usuarias de los servicios de comunicaciones. Esto contradice estándares internacionales que exigen que las interceptaciones y la retención de datos estén reguladas de manera detallada, con reglas claras sobre competencias, límites, umbrales de sospecha y su supervisión independiente.

Tanto el Relator Especial de la ONU, Martin Scheinin, como fallos internacionales, han insistido en que las leyes de inteligencia deben precisar con exactitud los supuestos que justifican medidas tan invasivas como la interceptación de comunicaciones. La normativa en cuestión debe establecer los objetivos perseguidos, los tipos de personas o actividades bajo vigilancia, los plazos de conservación de datos, y prever controles judiciales previos, así como mecanismos de supervisión y rendición de cuentas para evitar abusos. Los Principios Necesarios y Proporcionados (2013) refuerzan estas exigencias, destacando la legalidad, necesidad, proporcionalidad y control judicial de las medidas de vigilancia.

En contraste, la LOI y su Reglamento presentan vacíos significativos que afectan seriamente la legalidad de la norma, y por tanto la vuelven inconvencional de cara a estándares de derechos humanos. Aunque ambos cuerpos normativos mencionan tangencialmente los principios de necesidad y proporcionalidad, no explican cómo deben aplicarse en la práctica, ni fijan umbrales de sospecha para justificar la interceptación de las comunicaciones, ni prevén la posibilidad de su impugnación por parte de las empresas proveedoras de los servicios de telecomunicaciones. El Reglamento incluso delega a futuro en la autoridad del SNI la elaboración de lineamientos sobre la implementación operativa de las interceptaciones, lo que aumenta el riesgo de arbitrariedad y erosiona las garantías de protección de los derechos humanos.

Uno de los aspectos más problemáticos en la regulación de la interceptación de las comunicaciones es la obligación de retención de datos por hasta cinco años, lo que implica una conservación generalizada y excesivamente extensa de los metadatos de todas las personas usuarias de los servicios de telecomunicaciones, sin distinción. Experiencias comparadas, como la jurisprudencia del Tribunal de Justicia de la Unión

Europea, han señalado[68] que cuanto más prolongada sea la retención y más indiscriminada la recopilación, más grave es la injerencia en la privacidad. Además, la Corte IDH ha reconocido que los metadatos gozan de la misma protección que el contenido de las comunicaciones, dado su potencial para revelar aspectos íntimos de la vida de las personas[69].

En síntesis, el marco regulatorio de la LOI permite un acceso amplio y poco controlado a información altamente sensible, lo que representa una amenaza directa a los derechos a la privacidad y a la protección de datos. La ausencia de límites claros, de controles judiciales efectivos y de garantías frente a abusos convierte la regulación en incompatible con los estándares internacionales de derechos humanos, al habilitar una vigilancia masiva y desproporcionada que afecta no solo a personas investigadas, sino también a terceros vinculados a éstas.

VIII. 2. A Desarrollo de la argumentación

La Ley Orgánica de Inteligencia obliga a los proveedores de los servicios de telecomunicaciones a entregar un extenso conjunto de información de las personas usuarias de dichos servicios, sin que medien mecanismos para su protección o de carga argumentativa a cargo de la autoridad del SNI requirente de la misma (art. 51).

El Relator Especial de la ONU para los derechos humanos y la lucha contra el terrorismo, Martin Scheinin, sugiere en su informe de 2009 la necesidad de que las técnicas y métodos especiales de investigación, y en especial las interceptaciones de las comunicaciones, deban estar consagradas en la ley a través de disposiciones "sumamente detalladas".[70] Es decir, las facultades para el intercambio de datos e información, la interceptación y seguimiento de las comunicaciones, la obligación de retención y acceso a los datos de las personas usuarias de los servicios de telecomunicaciones, entre otros, deben constar en regulaciones específicas y exhaustivas que definan las competencias y atribuciones de las autoridades del sistema

[68] En los casos Digital Rights Ireland and Others (Joined Cases) (C-293/12) de 2013 y Tele2 Sverige AB v Post- och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Watson (C-698/16).
[69] Corte Interamericana de Derechos Humanos, Caso Escher y otros vs Brasil. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 6 de julio de 2009, párrafo 114 y siguientes
[70] Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la Promoción y la Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha Contra el Terrorismo, Martin Scheinin, A/HRC/10/3, del 4 de febrero de 2009, párrafos 27 y siguientes

de inteligencia.[71]

En el mismo tenor, el fallo CAJAR vs Colombia reiteró la importancia de que la legislación que regule sobre las tareas de inteligencia describa "**con la mayor precisión posible**":[72]

- Los tipos y medidas, así como acciones empleadas para la obtención y recopilación de información en materia de inteligencia,
- Los objetivos perseguidos a través de dichas medidas,
- Las clases de personas y actividades sobre las cuales se podrá obtener y recopilar información, en función de amenazas que deben ser identificadas con claridad y fines que buscan proteger esas actividades,
- El grado o el umbral de sospecha que puede justificar la recopilación y obtención de la información, en especial cuando se emplean métodos de interceptación de las comunicaciones,
- Los plazos aplicables a las tareas de recolección de información y uso de las técnicas y medios empleados, y
- Los métodos útiles para actualizar, supervisar, examinar, obtener y recopilar dicha información.

El Relator Especial de la ONU, Martin Scheinin, ahonda mucho más en la importancia de que las leyes de inteligencia describan con precisión cuál es el umbral o nivel de sospecha aceptable para justificar el despliegue de técnicas y métodos de recopilación de información, como la interceptación de las comunicaciones. En su opinión, es fundamental que los Estados fijen con claridad normativa los umbrales "cuyo desbordamiento por un organismo de inteligencia podría desencadenar toda una serie de actividades que invadan los derechos humanos".[73]

---

[71] Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la Promoción y la Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha Contra el Terrorismo, Martin Scheinin, A/HRC/10/3, del 4 de febrero de 2009, párrafos 27 y siguientes

[72]Corte Interamericana de Derechos Humanos, Caso Miembros de la Corporación José Alvear Restrepo vs Colombia. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 18 de octubre de 2023, párrafo 538

[73] Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la Promoción y la Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha Contra el Terrorismo, Martin Scheinin, A/HRC/10/3, del 4 de febrero de 2009, párrafo 31

Adicionalmente, los "Principios Necesarios y Proporcionados sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones"[74], confeccionados en 2013 por más de 40 personas expertas, y respaldada a nivel global por más de 400 organizaciones de la sociedad civil recuerdan la importancia de que medidas como la interceptación de las comunicaciones satisfaga los principios de legalidad, objetivo legítimo, necesidad, idoneidad y proporcionalidad (Principios 1 al 5).

Asimismo, prevén que una autoridad judicial competente, independiente e imparcial revise las órdenes de vigilancia para dar cuenta de su legalidad y apego al debido proceso (Principio 6 y 7), y proponen, entre otros, el deber estatal de supervisar de manera transparente e independiente (Principio 9 y 10) la actuación de las autoridades con facultades para la vigilancia de las comunicaciones, para que informen al público sobre su uso, alcance y técnicas empleadas para dicho fin, así como el número de órdenes de vigilancia de las comunicaciones –o interceptaciones- emitidas, aprobadas y rechazadas (Principio 9).

La redacción actual de la LOI y su reglamento contraviene los estándares vigentes en derechos humanos que resultan aplicables a las medidas de interceptación por dos razones. Por una parte, por su redacción insuficiente y la gravedad de los vacíos que habilitan la arbitrariedad estatal, y por otra, la adopción de medidas regresivas que se consideran injerencias arbitrarias en la privacidad, como la fijación de períodos excesivamente extensos para la retención de datos de las comunicaciones de las personas usuarias de dichos servicios.

Para ahondar en esta incompatibilidad vale la pena prestar atención a la literalidad del artículo 51 de la LOI que, en principio, prevé que la orden de interceptación de las comunicaciones debe estar "debidamente justificada", pero aquella no señala los requisitos que debe satisfacer la autoridad del SNI en la exposición de su carga argumental, ni el medio en que debe constar dicha orden que se considera "secreta", según el Reglamento de la Ley (art. 34). Más aún, el Reglamento no desarrolla criterios asociados a la motivación fundada y ni siquiera se refiere a ella, agregando que basta la orden de interceptación "sin que medie otro requisito adicional" (art. 34).

La LOI no refiere de ninguna manera la posibilidad de que los proveedores del servicio de telecomunicaciones puedan impugnar o oponerse a la orden de interceptación cuando la

[74] Necessary and Proportionate Coalition, Necesarios y Proporcionados (Versión de Mayo 2014). En: https://necessaryandproportionate.org/es/necesarios-proporcionados

consideren excesiva o infundada (art. 51, LOI). Omite asimismo cualquier alusión al umbral o nivel de sospecha que motivaría una orden de interceptación de las comunicaciones, y guarda silencio sobre la eventual existencia de mecanismos de supervisión de la orden (independientes o judiciales), su ejecución y resultados.

Pese a los vacíos que se advierten en disposiciones centrales para el marco jurídico de inteligencia, la redacción actual de la norma habilitaría al SNI a requerir acceso a un conjunto extenso y detallado de información, y por lo mismo, potencialmente crítico para los derechos a la privacidad de las personas usuarias de los servicios de telecomunicaciones (art. 51 LOI; art. 34 del Reglamento).

Entre el vasto conjunto de información que puede solicitar y acceder dicha autoridad, se menciona en el artículo 51 de la LOI los siguientes ítems que desagregamos para mayor claridad, así:

- Datos de las comunicaciones:
    - Acceso a las comunicaciones en tiempo real.
- Metadatos de las comunicaciones:
    - Información histórica del abonado celular,
    - Información de conexión de los abonados –es decir, información precisa desde donde y con quiénes se comunican-,
    - Información técnica e informática –es decir, desde qué dispositivos, y qué tipo de comunicaciones sostienen, así como qué tipo de contenidos intercambian[75],
    - Localización de las celdas donde se encuentran las terminales[76] y,
    - En general, todo tipo de información –según la literalidad de la LOI– que facilite la identificación y localización del abonado celular en cuestión.

Este listado refiere a un volumen de información con un amplio potencial invasivo de la

[75] Es decir, información sobre si las comunicaciones fueron sostenidas por telefonía o por VoIP, es decir, llamadas de video o telefónicas habilitadas a través del acceso a internet. Así como metadatos asociados a los tipos de contenidos que se intercambian a través de aplicativos o servicios de comunicación –imágenes, video, texto o audio–.

[76] Es decir, información que permite geolocalizar o posicionar geográficamente la ubicación de un dispositivo a través de la triangulación en la conexión efectuada por las torres de comunicaciones.

privacidad no solo de las personas objetivo de las tareas de inteligencia sino de terceras vinculadas a estas, pues permiten obtener un grado de detalle minucioso y continuo tanto sobre el contenido de las comunicaciones como sobre los metadatos asociados a estas. Es decir, tanto las palabras y expresiones usadas como aquellos elementos de la comunicación que, al informar sobre las ubicaciones, los dispositivos involucrados y los momentos de una comunicación, dan cuenta, por ejemplo, sobre los hábitos de las personas, los lugares de tránsito y destino que frecuentan, sus redes de interacción social, familiar y conocidos, sus actividades culturales y laborales, así como otros aspectos más sensibles como el estado de salud, las opiniones sobre temas políticos o sensibles, entre otros.

Por su parte, el artículo 51 de la LOI, realiza una mención meramente formal a que se "deberán observar los principios de necesidad y proporcionalidad, evitando en todo momento su aplicación arbitraria". Sin embargo, el artículo que autoriza las interceptaciones de las telecomunicaciones omite por completo el desarrollo específico, exhaustivo y detallado de cómo serían operacionalizadas en la práctica dichas garantías para la protección de las personas y la prevención de abuso de dicha facultad. En consecuencia la referencia a estos principios, sin mayores precisiones, permanece en un plano meramente declarativo y carece de eficacia real.

Si bien el Reglamento de la LOI debería haber abordado esas materias, al igual que en la regulación de la entrega de información en manos de entidades públicas, privadas y naturales, éste hace una delegación regulatoria futura en donde encarga a la autoridad del SNI para que, con posterioridad, delimite los lineamientos aplicables a (i) la implementación operativa de la interceptación de las comunicaciones, (ii) lineamientos de seguridad de la información y (iii) sobre la periodicidad de "los reportes" a los que se refiere el enunciado normativo, sin mayor contexto sobre qué tipo de reportes se trata, cuál es su naturaleza o quién debe confeccionarlos para informar sobre qué tipo de asunto (art. 34, Reglamento).

En todo caso, la regulación futura que deberá expedir la autoridad del SNI no contempla lineamientos destinados a preservar la privacidad de la ciudadanía frente a intromisiones arbitrarias o ilegales, ni establece cómo deberían de ser operativizadas las órdenes de interceptación para garantizar el respeto de los principios de proporcionalidad y necesidad referidos en el art. 51 de la LOI. Tampoco prevé mecanismos claros para prevenir, detectar o remediar eventuales usos arbitrarios de dicha facultad legal.

VII. 2. B Sobre la obligación de retención de datos de las personas suscriptoras

Particularmente la LOI (art. 51) faculta a las autoridades de los subsistemas de inteligencia militar y policial a solicitar información de las personas suscriptoras de los servicios de telecomunicaciones por un período máximo de cinco (5) años. Esta disposición crea, sin advertirlo expresamente, la obligación de retención o almacenamiento de metadatos a cargo de las empresas proveedoras de dichos servicios.

Es decir, las empresas se verán en la obligación de conservar por hasta cinco años copia de todo el conjunto de metadatos asociados a las comunicaciones de las personas usuarias (descritos en el primer párrafo del art. 51 de la LOI), y que eventualmente puedan ser de interés de las autoridades de los subsistemas del SNI. Es importante destacar que los metadatos de las comunicaciones –y su retención– configuran hoy en día uno de los insumos y mecanismos principales que articulan y facilitan la vigilancia masiva del Estado sobre las personas.[77]

En esta disposición plantea dos problemas centrales desde la perspectiva de protección a la privacidad y seguridad de las personas: el plazo aplicable a la retención de datos, y la obligación de retención generalizada sobre un conjunto indiscriminado de datos que pesa sobre la totalidad de los personas usuarias de los servicios de telecomunicaciones.

En cuanto al plazo, la retención de datos de las personas suscriptoras de los servicios de telecomunicaciones ha sido objeto de controversia en diversas jurisdicciones[78] donde se ha determinado que, cuanto más prolongado sea el período de conservación, más intensa resulta la injerencia arbitraria en la privacidad de las personas.

La razón de dicha injerencia, según diversas decisiones del Tribunal de Justicia de la Unión Europea[79] (TJUE), así como la opinión de organizaciones de la sociedad civil

[77] Ver: Alena Birrer, Danya He, Natascha Just (2023). The state is watching you—A cross-national comparison of data retention in Europe, *Telecommunications Policy*, Vol 47, Nº 4, en: https://www.sciencedirect.com/science/article/pii/S0308596123000538 ; Valsamis Mitsilegas, Elspeth Guild, Elif Kuskonmaz, Niovi Vavoula (2022). Data retention and the future of large-scale mass surveillance: The evolution and contestation of judicial benchmarks, *European Law Journal*, Vol 29, pp 176-211, en: https://onlinelibrary.wiley.com/doi/epdf/10.1111/eulj.12417

[78] Los casos de disputa legal más conocidos en este sentido han tenido lugar en la Unión Europea, con decisiones en los casos Digital Rights Ireland and Others (Joined Cases) (C-293/12) de 2013 y Tele2 Sverige AB v Post- och telestyrelsen (C-203/15); Secretary of State for the Home Department v. Watson (C-698/16).

[79] Ídem

expertas en la materia como Privacy International[80] o European Digital Rights[81], se debe a que la conservación de dichos registros puede habilitar a búsquedas con un contenido histórico y contextual tan detallado e invasivo que conduce al riesgo de inferencias excesivas o desproporcionadas sobre las personas, a su perfilamiento y escrutinio excesivo de sus vidas privadas. Por tanto, la conservación de metadatos por las empresas proveedoras de los servicios de telecomunicaciones debe ser tan limitada como sea posible, para que los registros entregados a las autoridades no solo sean más recientes, sino más acotados.

En la Unión Europea, por ejemplo, los períodos de retención de metadatos de las comunicaciones oscilan entre los 6 meses y hasta los 24 meses como período máximo permitido,[82] en atención al contenido de la Directiva Europea de Retención de Datos que, aunque fue invalidada por el TJUE –por imponer, entre otros, una obligación abstracta de retención de todos los metadatos de todas las personas suscriptoras de los servicios de telecomunicaciones–, y que fue recogida en las legislaciones nacionales de los países de la Unión cuyo contenido, en su mayoría, se sigue alineando a los plazos fijados en 2006 por dicha Directiva.[83]

Por otro lado, el Tribunal de Justicia de la Unión Europea también ha reiterado en diferentes decisiones[84] que la eventual injerencia sobre la privacidad no solo se refiere a los aspectos temporales de la medida de retención de metadatos, sino especialmente a la naturaleza generalizada de los registros que deben ser retenidos por las empresas de telecomunicaciones, es decir, a la obligación de que retengan de manera indiscriminada

[80] Ver: Privacy International (2017). A concerning State of Play for the Right to Privacy in Europe. National Data Retention Laws since the CJEU's Tele-2/Watson Judgment. En: https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf

[81] European Digital Rights EDRi (2021). Europe's Data Retention Saga and its risks for Digital Rights. En: https://edri.org/our-work/europes-data-retention-saga-and-its-risks-for-digital-rights/

[82] Esto ha sido fijado así por la Directiva Europea de Retención de Datos de 2006, que ordena la retención entre 6 a 24 meses con fines enfocados en la persecución e investigación de delitos. Dicha Directiva fue cuestionada ante el Tribunal de Justicia de la Unión Europea (CJEU por su siglas en inglés) en el caso "Digital Rights Ireland and Others" que la declaró inválida por considerarla una invasión arbitraria de la privacidad. La invalidez se fundó en la desproporcionalidad que significa la retención intensiva y generalizada de todo tipo de metadatos de personas usuarias de los servicios de telecomunicaciones. Esta decisión ha sido reiterada también en Tele2 Sverige AB v Post- och telestyrelsen (C-203/15) and Secretary of State for the Home Department v. Watson (C-698/16).

[83] European Union Agency For Fundamental Rights FRA (2019). Data retention across the EU. En: https://fra.europa.eu/en/publication/2017/data-retention-across-eu

[84] Como *Digital Rights and Others; Tele2 Sverige AB v Post- och telestyrelsen* (C-203/15) y *Secretary of State for the Home Department v. Watson* (C-698/15), donde el Tribunal decidió que los Estados no podían imponer obligaciones generales de retención de datos a las empresas de telecomunicaciones y aclaró que solo podría imponerse para fines específicos, como la persecución e investigación de algunos de los delitos más graves, entre otros.

diversos tipos de metadatos de las personas usuarias.

Precisamente en la decisión *Digital Rights Ireland*, la primera del TJUE en esta materia y que condujo a la invalidación de la Directiva sobre Retención de Datos, se afirmó que la obligación de retención generalizada de todo el tráfico de las comunicaciones, es decir, de todas las personas –con y sin investigaciones criminales pendientes–, y metadatos obtenidos de todas las formas de comunicación sin ninguna distinción, limitación o excepción, resulta desproporcionada y, por tanto, una injerencia arbitraria en el derecho a la privacidad. También reiteró en dicho fallo que la medida de retención solo resulta proporcional y necesaria para la persecución de los más graves crímenes, como el de terrorismo. Y enfatizó en la importancia de que las medidas de retención de datos contengan mecanismos efectivos para la protección de los datos personales de los personas usuarias de los servicios de telecomunicaciones, así como mecanismos para su defensa en caso de abuso, uso o acceso ilegal a dichos registros.

Precisamente, la ausencia de estos mecanismos de resguardo, así como el alcance generalizado de la medida de retención, fueron los motivos que condujeron a la invalidación de la Directiva en tanto que incompatible con el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales.[85]

Sobre la capacidad intrusiva de la retención de metadatos de las comunicaciones, la Oficina del Alto Comisionado para los Derechos Humanos ha adoptado posturas mucho más contundentes, al afirmar que no debe existir distinción entre la protección concedida al contenido de las comunicaciones y la protección sobre los metadatos que tienen igual o mayor capacidad intrusiva sobre la privacidad:[86]

> "(...) se ha sugerido que la interceptación o la recopilación de datos acerca de una comunicación, en contraposición al contenido de la comunicación, no constituyen en sí mismas una injerencia en la vida privada. Desde el punto de vista del derecho a la privacidad, esa distinción no es convincente. La agregación de la información comúnmente conocida como **"metadatos" puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la**

[85] Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, C-293/12 y C-594/12. En: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293

[86] Consejo de Derechos Humanos, Reporte de la Oficina del Alto Comisionado para los Derechos Humanos, "El Derecho a la Privacidad en la era digital", A/HRC/27/37, del 30 de junio de 2014, párrafo 19

identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada.

"Como observó recientemente el Tribunal de Justicia de la Unión Europea, los metadatos de las comunicaciones, "considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado". (Énfasis propio)

De hecho, dicha Oficina ha identificado en distintos reportes tres tendencias predominantes en las regulaciones sobre retención de datos.[87] La primera es la retención obligatoria de distintos tipos de metadatos sin justificación ni limitación, únicamente ante la eventual posibilidad de que las autoridades llegasen a tener interés en su consulta o acceso a futuro; la segunda es un exceso de dependencia de las autoridades en el acceso y consulta de dicha información, lo que resulta perjudicial para la privacidad, y en muy escasas ocasiones, necesaria o proporcionada; y la tercera, es una tendencia al abuso de las facultades asociadas a la acceso a los metadatos y la evasión de procedimientos que buscan proteger a las personas afectadas.

Más aún, esta parece ser en palabras de dicho organismo, una política pública de los regímenes de inteligencia característica de los Estados inclinados a la vigilancia masiva[88]. Por lo que la mera captura y retención de metadatos por las empresas de telecomunicaciones –sea que las autoridades los lleguen a consultar o no–, resulta en sí misma en una interferencia arbitraria del derecho a la privacidad.[89]

De vuelta al artículo 51 de la LOI que aborda esta materia –a diferencia del Reglamento, que guarda silencio sobre este punto– su contenido resulta deficiente pues (i) no explicita las razones por el espectro temporal de la retención de datos de hasta cinco años, (ii) contiene un deber de retención generalizado de un grupo extenso e indiscriminado de metadatos, y (iii) no consagra ninguna garantía en protección de la privacidad y protección de datos de las personas.

Sobre este asunto, el Relator Especial, Martin Scheinin, advirtió por su parte sobre el riesgo asociado a plazos extensos de retención de datos de las personas usuarias de los

[87]Consejo de Derechos Humanos, Reporte de la Oficina del Alto Comisionado para los Derechos Humanos, "El Derecho a la Privacidad en la era digital", A/HRC/51/17 del 4 de agosto de 2022, párrafo 41

[88] Consejo de Derechos Humanos, Reporte de la Oficina del Alto Comisionado para los Derechos Humanos, "El Derecho a la Privacidad en la era digital", A/HRC/27/37 del 30 de junio de 2014, párrafo 26

[89] Consejo de Derechos Humanos, Reporte de la Oficina del Alto Comisionado para los Derechos Humanos, "El Derecho a la Privacidad en la era digital", A/HRC/27/37 del 30 de junio de 2014, párrafo 20.

servicios de telecomunicaciones y que, en general, suelen tener una protección constitucional más limitada por visiones obsoletas que sugieren diferencias entre el contenido de las comunicaciones –que suelen merecer una protección más intensa–, en comparación con los datos y metadatos de las comunicaciones por ser supuestamente menos invasivos.[90]

Al respecto, vale la pena reiterar que, de conformidad al fallo Escher y otros vs Brasil, la Corte IDH señaló que los metadatos de las comunicaciones también se encuentran protegidos por el derecho a la vida privada consagrado en la Convención Americana sobre Derechos Humanos, al expresar que:

> Como esta Corte ha señalado anteriormente, aunque las conversaciones telefónicas no se encuentran expresamente previstas en el artículo 11 de la Convención, se trata de una forma de comunicación incluida dentro del ámbito de protección de la vida privada. El artículo 11 protege las conversaciones realizadas a través de las líneas telefónicas instaladas en las residencias particulares o en las oficinas, sea su contenido relacionado con asuntos privados del interlocutor, sea con el negocio o actividad profesional que desarrolla. De ese modo, **el artículo 11 se aplica a las conversaciones telefónicas independientemente de su contenido e incluso, puede comprender tanto las operaciones técnicas dirigidas a registrar ese contenido, mediante su grabación y escucha, como cualquier otro elemento del proceso comunicativo mismo**, por ejemplo, el destino de las llamadas que salen o el origen de las que ingresan, la identidad de los interlocutores, la frecuencia, hora y duración de las llamadas, aspectos que pueden ser constatados sin necesidad de registrar el contenido de la llamada mediante la grabación de las conversaciones. En definitiva, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación.[91] (Énfasis propio)

La distinción entre la protección que merece el contenido de las comunicaciones, y los

[90] Consejo de Derechos Humanos de las Naciones Unidas, Informe del Relator Especial sobre la Promoción y la Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha Contra el Terrorismo, Martin Scheinin, A/HRC/13/37, del 28 de diciembre de 2009, párrafo 42 y siguientes.
[91] Corte Interamericana de Derechos Humanos, Caso Escher y otros vs Brasil. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 6 de julio de 2009, párrafo 114 y siguientes

metadatos de las comunicaciones, resulta entonces en palabras del Relator Especial, en una diferenciación enturbiada de cara al estado del arte tecnológico que facilitaría explotar los datos de las comunicaciones de formas que resultan invasivas de la privacidad, por lo que se precisa de garantías legales robustas también para este tipo de información.

Por tanto, solicitamos a esta honorable Corte Constitucional que declare la inconstitucionalidad del artículo 51 de la LOI y del art. 34 del Reglamento en tanto que su apertura, vaguedad e imprecisión, habilita a injerencias arbitrarias sobre el ejercicio del derecho a la privacidad del que son titulares las personas usuarias de los servicios de telecomunicaciones, además de que atentan en su redacción actual contra el principio de legalidad, volviéndolas incompatibles con los estándares en derechos humanos a nivel universal e inconvencionales con los de alcance regional.

VII. 3. Derecho a la privacidad / Art. 43 de la LOI sobre vigilancia del espectro electromagnético y el ciberespacio

La Ley de Inteligencia contempla el uso de tecnologías para vigilar el espectro electromagnético y el ciberespacio, pero no desarrolla límites claros ni establece controles efectivos. Por su parte, el Reglamento guarda silencio sobre los alcances o límites de dicha facultad. Esta omisión abre la puerta a prácticas de vigilancia masiva e indiscriminada, comparables a la llamada “pesca milagrosa”, que afectan a miles de personas sin relación con amenazas concretas contra la seguridad del Estado.

En el caso del ciberespacio, la recolección de información mediante técnicas y metodologías tipo OSINT y SOCMINT, junto con el cruce eventual con otras bases de reconocimiento facial, migratorias o de videovigilancia, incrementaría la capacidad de perfilamiento y control sobre la ciudadanía, con graves implicaciones para la privacidad, la libertad de expresión y la participación política en un entorno democrático.

La sociedad civil y la academia han documentado cómo estas herramientas, utilizadas en América Latina, se aplican de manera desproporcionada y sin límites legales claros, normalizando la vigilancia permanente de las personas en línea. El Consejo de Derechos Humanos de la ONU ha advertido que el monitoreo generalizado del espacio digital es casi siempre desproporcionado y exige a los Estados marcos normativos estrictos, transparencia y mecanismos de supervisión.

En este contexto, la vigilancia masiva no solo erosiona la privacidad digital, sino que

también genera consecuencias jurídicas y sociales, como la estigmatización por la actividad en redes, la inclusión indefinida en bases de datos de inteligencia y la falta de seguridad jurídica frente a estas prácticas.

VII. 3. A Desarrollo de la argumentación

Asimismo, la LOI prevé el uso de tecnologías, hardware y software, para "recopilar, analizar y utilizar" datos e información para generar información de inteligencia y contrainteligencia obtenida del espectro electromagnético y el ciberespacio (art. 43, LOI).

La LOI no desarrolla con mayor detalle las implicaciones de estas acciones que articulan tareas de vigilancia del espectro electromagnético y del ciberespacio, y el Reglamento no aborda esta materia, lo cual deja al arbitrio de las autoridades su aplicación vaga e imprecisa, favoreciendo el abuso de una facultad por sí misma excepcional e invasiva de la privacidad de las personas.

Entendemos que la vigilancia sobre el espectro electromagnético, esa autopista invisible por la que viajan las comunicaciones, es otra forma de sugerir que el Estado podrá hacer escuchas pasivas de las comunicaciones de personas indeterminadas. Se trata, en definitiva, de una modalidad más de vigilancia masiva con implicaciones para la privacidad equiparables a las de interceptación directa de las comunicaciones. Así lo han señalado diversas organizaciones de la sociedad civil, por ejemplo en el contexto colombiano, donde la Ley de Inteligencia faculta a las autoridades de inteligencia a monitorear el espectro, práctica que ha sido ampliamente cuestionada por su carácter invasivo.[92]

A esta práctica también se le denomina "pesca milagrosa", ya que no se dirige a interceptar las comunicaciones de alguien identificado o identificable, y que representa una amenaza concreta para "la soberanía y la seguridad del Estado". Por el contrario, se utiliza para rastrear entre cientos o miles de comunicaciones legítimas y privadas, con el fin de detectar si surge o no alguna amenaza que llame la atención de las autoridades. En consecuencia, por sus características, la vigilancia indiscriminada del espectro sacrifica

[92] Privacy International (Agosto, 2015). Un estado en la sombra: vigilancia y orden público en Colombia. Informe Especial. Disponible en: https://www.privacyinternational.org/sites/default/files/2017-12/ShadowState_Espanol.pdf

de manera arbitraria la privacidad de las personas que no guardan relación alguna con objetivos de inteligencia previamente identificados por el Estado.

Por su parte, la vigilancia del ciberespacio entraña por sí mismo el despliegue de tecnologías y técnicas de vigilancia de internet que pueden resultar excesivas o desproporcionadas para las personas usuarias de internet, como el uso de inteligencia en fuentes abiertas (OSINT, por sus siglas en inglés) e inteligencia en redes sociales (SOCMINT, por sus siglas en inglés), que ya ha sido empleada[93] por otras autoridades de inteligencia de la región.[94] De hecho, el Reglamento explicita que se podrá desplegar inteligencia en fuentes abiertas en el art. 16, entre otras modalidades de inteligencia incluidas las de Señales (SIGINT) y de imágenes (IMINT) y que diversifican la caja de herramientas del Estado para vigilar a la ciudadanía en línea.

La documentación elaborada por la sociedad civil[95] y la academia[96] en la región sobre el uso de ese tipo de tecnologías, técnicas y herramientas para la vigilancia de internet, sugiere que para las autoridades de inteligencia en la práctica no hay límites al monitoreo o perfilamiento de personas en internet, en tanto que los datos e información que circula en línea son de supuesto libre uso y acceso por el mero hecho de su publicación. Desde luego, la LOI se refiere de manera apenas tangencial y vaga a la vigilancia del ciberespacio que será desplegada por la autoridad encargada del SNI, lo que aumenta los riesgos de abuso e injerencias ilegales a la protección del derecho a la privacidad en línea.

Como fue sostenido al principio de este *amicus*, la privacidad es un derecho que debe ser

---

[93] Camacho, L.; Ospina, D.; Upegui, J.C. (2023). Inteligencia estatal en internet y redes sociales: la privacidad bajo amenaza. Disponible en: https://www.dejusticia.org/publication/inteligencia-estatal-en-internet-y-redes-sociales-la-privacidad-bajo-amenaza/

[94] Zara, N. (2023). Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay. Disponible en: https://www.palermo.edu/Archivos_content/2023/cele/papers/233008-reporte-regional-OSINT.pdf

[95] Camacho, L.; Ospina, D.; Upegui, J.C. (2023). Inteligencia estatal en internet y redes sociales: la privacidad bajo amenaza. Disponible en: https://www.dejusticia.org/publication/inteligencia-estatal-en-internet-y-redes-sociales-la-privacidad-bajo-amenaza/ ; Fundación Karisma (2023). OSINT. Imagina que hay un policía que ve todo lo que haces en internet. Disponible en: https://web.karisma.org.co/osint/

[96] Bertoni, E. (2023). Las prácticas OSINT, ¿son amigas o enemigas de los derechos humanos?. Centro de Estudios para la Libertad de Expresión CELE. Disponible en: https://www.palermo.edu/Archivos_content/2023/cele/papers/231115-Bertoni-reporte-inicial-OSINT.pdf ; Zara, N. (2024). OSINT e inteligencia artificial: una mirada regional sobre una combinación explosiva. Centro de Estudios para la Libertad de Expresión CELE. Disponible en: https://observatoriolegislativocele.com/osint-e-inteligencia-artificial-una-mirada-regional-sobre-una-combinacion-explosiva-por-nicolas-zara/

garantizado en línea como fuera de ella, por lo que su alcance de protección y estándares deben conservar vigencia también frente a la modalidad de las tareas de inteligencia que se despliegan en internet o en el ciberespacio.

En nuestro informe "Perfilamiento en redes sociales y ciberpatrullaje como nuevas modalidades de la vigilancia masiva desplegada por los Estados: casos relevantes en América Latina"[97], enfocado en la inteligencia estatal en internet que se operacionaliza con el uso de metodologías y herramientas de OSINT y SOCMINT, expresamos que:

> En el seno del Consejo de Derechos Humanos se aprobó en 2022 el informe sobre "el derecho a la privacidad en la era digital" que, por primera vez, explora las prácticas de inteligencia en redes sociales SOCMINT y de monitoreo del discurso en línea como nuevas modalidades de la vigilancia masiva en internet desplegadas por los Estados.
>
> Sobre el monitoreo y la inteligencia en redes sociales, sostuvo que son prácticas que tienen un serio impacto en los derechos humanos. Por ejemplo, el uso de tecnologías digitales que facilitan ambas tareas puede dar un mayor alcance y escala al monitoreo que puede tener fines legítimos o ilegítimos.
>
> Más aún, esta amenaza se agrava cuando las fuentes de información obtenidas de las redes sociales son cruzadas con otras bases de datos, como las de reconocimiento facial y videovigilancia –también a disposición de los Estados– la información que reposa en manos de los proveedores de servicios de internet, las bases de datos de migrantes, incluso las que son armadas para perfilar a opositores políticos, lo que magnifica la capacidad de la vigilancia masiva y en tiempo real de la que éstos disponen.
>
> Las amenazas del monitoreo en línea y la inteligencia en redes sociales son múltiples. Ponen en riesgo el ejercicio del derecho a la libertad de expresión, a la reunión pacífica, a la participación en entornos en línea y fuera de ella. Al respecto, la resolución afirma que "individuals should have a space free from systematic

[97] Derechos Digitales (Agosto, 2024). Perfilamiento en redes sociales y ciberpatrullaje como nuevas modalidades de la vigilancia masiva desplegada por los Estados: casos relevantes en América Latina. Contribución de Derechos Digitales para la consulta "sobre tecnologías de vigilancia digital y derechos humanos" emprendida por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos CIDH. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/Informe-RELE-vigilancia-masiva_cerrado.pdf página 28

observation and intrusion, in particular by government entities"/ "las personas deberían tener un espacio libre de la sistemática observación e intrusión, en especial de las entidades gubernamentales".

Asimismo, la **resolución sostiene que el monitoreo general del espacio público digital y fuera de línea es casi siempre desproporcionado**. Y recomendó a los Estados adoptar marcos legales adecuados para regular la recolección, análisis y compartición de inteligencia obtenida de redes sociales que delimite claramente los escenarios en que ésta se encuentra permitida, sus prerrequisitos, las autorizaciones y procedimientos, así como los mecanismos para garantizar su supervisión adecuada. (Énfasis propio).

Entre las múltiples consecuencias que pueden desprenderse la inteligencia estatal que se despliega en internet, identificamos en dicho informe las siguientes:[98]

- La generación de consecuencias jurídicamente relevantes sobre las personas en razón a su actividad en internet y la consecuente estigmatización derivada de sus comentarios, seguidores o lista de seguidos, preferencias, retuits, me gusta u otro tipo de republicación o interacción en línea,
- La "extensión indeterminada en el tiempo de la vigilancia masiva sobre las personas", es decir, su inclusión indefinida en bases de datos de "sujetos de interés" que son elaboradas en el marco de las tareas de inteligencia, y la eventual instrumentalización de esta información con repercusiones para el ejercicio de derechos, no solo el de la privacidad, sino la libertad de expresión, de asociación, entre otros,
- La ausencia de seguridad jurídica asociada a estas prácticas, su transparencia y legalidad.

Volviendo al contenido de la LOI, reiteramos cómo la abierta vigilancia del espectro electromagnético y del ciberespacio sin mayores precisiones normativas ni salvaguardas, favorece un escenario de abuso y vulneración sistemática de la privacidad de las

[98] Derechos Digitales (Agosto, 2024). Perfilamiento en redes sociales y ciberpatrullaje como nuevas modalidades de la vigilancia masiva desplegada por los Estados: casos relevantes en América Latina. Contribución de Derechos Digitales para la consulta "sobre tecnologías de vigilancia digital y derechos humanos" emprendida por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos CIDH. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/Informe-RELE-vigilancia-masiva_cerrado.pdf página 29

personas. Las prácticas de inteligencia estatal, en particular el monitoreo de redes sociales y el perfilamiento en línea, amplifican la capacidad de los Estados para desplegar vigilancia masiva con serias consecuencias para los derechos humanos, tal y como advertimos en dicho informe.

Frente a ello, resulta indispensable exigir la adecuación de la normativa nacional a los estándares internacionales de derechos humanos, estableciendo límites claros, controles efectivos y mecanismos de supervisión independientes. Solo así se podrá garantizar que la inteligencia estatal no derive en una intrusión arbitraria que, en nombre de la seguridad, sacrifique el derecho fundamental a la privacidad y otras libertades esenciales en una sociedad democrática.

Por tanto, solicitamos de manera respetuosa a esta honorable Corte Constitucional que declare la inconstitucionalidad del artículo 43 de la LOI por no satisfacer con suficiencia el principio de legalidad, pues su contenido habilita a injerencias arbitrarias que limitan el derecho a la privacidad, poniendo en riesgo con su vaguedad, amplitud e indeterminación enunciativa, el principio democrático de seguridad jurídica.

VII. 4 Derecho a la protección de datos personales en el marco de las tareas de inteligencia y contrainteligencia / Arts. 31 y 32 del Reglamento

La Ley Orgánica de Inteligencia y su Reglamento no establecen reglas claras de protección de datos en actividades tan delicadas como la interceptación de comunicaciones, la vigilancia del ciberespacio o el intercambio de información entre entidades públicas y privadas. Esta ausencia es preocupante, pues la Corte IDH, en el caso CAJAR vs. Colombia, reconoció expresamente que el derecho a la protección de datos debe aplicarse en el ámbito de la inteligencia.

En ese fallo, la Corte señaló que cuando se recopilan y almacenan datos personales en tareas de inteligencia deben existir políticas claras que indiquen quién es responsable de la información, con qué propósito se procesa, cuál es la base legal para hacerlo, cuánto tiempo se conservarán los datos, qué técnicas se emplean y quién accede a ellos. Además, estableció que las personas tienen derecho a solicitar la cancelación, actualización o eliminación de sus datos incluidos en archivos de inteligencia.

Sin embargo, ni la LOI ni su Reglamento recogen estos estándares, y la Ley de Protección de Datos de 2021 tampoco aplica a las labores de inteligencia, aunque reconoce que

cualquier norma futura sobre seguridad nacional debe ajustarse a criterios de legalidad, necesidad y proporcionalidad.

El Reglamento creó una "Unidad de protección de datos de inteligencia y contrainteligencia", pero sus funciones se limitan a controlar el flujo de información en las bases de datos y evitar el almacenamiento de categorías sensibles. No reconoce derechos como la rectificación, cancelación o eliminación de datos personales, lo que la aleja de los estándares internacionales y podría hacer que su contenido sea considerado inconvencional.

VII. 4. A Desarrollo de la argumentación

La Ley Orgánica de Inteligencia y el Reglamento carecen de previsiones asociadas a la protección de datos en el marco de las tareas de inteligencia, las cuales deberían de regir especialmente en las situaciones de entrega y solicitud de datos e información en manos de entidades públicas y privadas; en los procesos de interceptación de las comunicaciones; y en la vigilancia del ciberespacio.

El fallo CAJAR vs. Colombia, referido a lo largo de esta presentación, reconoció por primera vez la aplicación del derecho a la protección de datos en el marco de las tareas de inteligencia en dos situaciones. La primera, asociado a los datos personales contenidos en los archivos de inteligencia; y la segunda, a la protección de datos personales en el proceso de recolección de información de inteligencia.

En dicho fallo, la Corte IDH estableció que, cuando la recopilación y almacenamiento de información de inteligencia involucra el procesamiento de datos personales, se deben crear disposiciones para crear políticas de protección de datos que permitan mantener registros que identifiquen: (i) los responsables de la información recopilada, (ii) los propósitos para el procesamiento de la información recopilada, indicando el origen y categoría de los datos, (iii) la base jurídica de las operaciones realizadas, (iv) los plazos de conservación de la información, (v) las técnicas utilizadas para el tratamiento de la información, así como (vi) registros cronológicos de acceso, alteración, consulta, eliminación o divulgación de los registros cuando contengan datos personales, y registro de las personas que accedieron a estos.[99]

[99]Corte Interamericana de Derechos Humanos, Caso Miembros de la Corporación José Alvear Restrepo vs Colombia. Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 18 de octubre de 2023, párrafo 540

Las reglas que orienten la protección de datos aplicables a las tareas de inteligencia, deben estar proyectadas no solo en relación con el tratamiento de datos contenidos en la "información accionable" de inteligencia, sino también a los archivos de inteligencia en los que esos datos terminan incorporándose. Sobre tales archivos, la jurisprudencia referida reconoció expresamente el derecho que tienen los titulares de los datos a ejercer el derecho a la cancelación, actualización o eliminación de los mismos.[100]

Llamamos la atención sobre el hecho de que la LOI y su Reglamento guardan absoluto silencio respecto a estas materias vinculadas a la protección de datos personales, las cuales tampoco son abordadas por la reciente Ley Orgánica de Protección de Datos aprobada en 2021, que no es aplicable sobre las tareas de inteligencia. Cabe destacar, además, que dicha ley prevé que la futura creación de reglas para la protección de datos en el ámbito de la seguridad nacional deberá, en todo caso, cumplir "estándares en derechos humanos y los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad" (artículo 11).

Es cierto que el Reglamento crea la "Unidad de protección de datos de inteligencia y contrainteligencia" (art. 31), y regula sus funciones (art. 32). Pero dicha unidad tiene la vocación exclusiva, según el artículo 32, de "controlar el ingreso y salida de información de bases de datos de inteligencia", verificar que no se almacenen categorías de datos sensibles, y delinear acciones para el intercambio de información entre los subsistemas del SNI.

El Reglamento no tiene como enfoque la articulación de los derechos de cancelación, actualización, corrección o eliminación de los que trata el fallo CAJAR vs. Colombia que operacionalizan en la práctica el ejercicio del derecho a la autodeterminación informativa en el marco de las tareas de inteligencia. Situación que haría inconvencional su contenido.

Por tanto, solicitamos de manera respetuosa a esta honorable Corte Constitucional que declare la inconstitucionalidad de los artículos 31 y 32 del Reglamento en razón a su inconvencionalidad, pues su redacción actual no satisface con suficiencia el estándar fijado en el fallo CAJAR vs. Colombia sobre protección del derecho a la autodeterminación

[100] Camacho, L. (2024). Histórica sentencia de la Corte Interamericana de Derechos Humanos: la protección de datos aplica en las tareas de inteligencia. Derechos Digitales. Disponible en: https://www.derechosdigitales.org/recursos/historica-sentencia-de-la-corte-interamericana-de-derechos-humanos-la-proteccion-de-datos-aplica-en-las-tareas-de-inteligencia/

informativa y protección de datos en el marco de las tareas estatales de inteligencia.

VII. 5 Derecho de acceso a la información pública y transparencia / Art. 13, 14, 43 de la LOI

La Ley Orgánica de Inteligencia (LOI) consagra la opacidad como regla general, colocando el secreto y la reserva por encima del derecho de la ciudadanía a fiscalizar el actuar del Estado en materia de inteligencia. La norma establece que prácticamente toda la información del Sistema Nacional de Inteligencia (SNI) es clasificada, lo que impide el escrutinio público y limita de manera extrema los contrapesos democráticos.

Incluso en aspectos sensibles como la adquisición de tecnologías de vigilancia, la ley prohíbe a cualquier autoridad revisar o cuestionar el uso de los recursos, blindando al SNI de cualquier control real. Las únicas excepciones –a saber, la revisión parcial de gastos por la Contraloría y la rendición condicionada ante la Asamblea Legislativa– son tan restringidas que resultan ineficaces para prevenir abusos, corrupción o violaciones de derechos humanos.

Este modelo de secretismo absoluto contrasta con los estándares interamericanos, que establecen el principio de máxima divulgación y solo permiten restricciones específicas, necesarias y proporcionales en contextos democráticos. Al no superar este test, la LOI resulta incompatible con el marco de derechos humanos vigente.

Los Principios de Tshwane, reconocidos por la CIDH, ofrecen una guía clara para equilibrar seguridad nacional y transparencia, obligando a los Estados a divulgar información clave: violaciones a los derechos humanos, marcos normativos sobre vigilancia, presupuestos de inteligencia, estadísticas de solicitudes de vigilancia de comunicaciones, entre otros. Sin embargo, la LOI ignora estas obligaciones y refuerza un manto de opacidad que favorece la discrecionalidad y el abuso.

VII. 5. A Desarrollo de la argumentación

La tensión entre la transparencia y la seguridad nacional suele hacer de la opacidad una regla general en las leyes de inteligencia, inhabilitando y obstaculizando el derecho legítimo de la ciudadanía y otras autoridades de escrutar las actuaciones del Estado cuando este ejerce facultades que pueden restringir de manera injustificada el ejercicio de derechos.

La LOI reitera en diversas ocasiones y de manera sostenida a lo largo del articulado que

las actividades y la información en manos de la autoridad del Sistema Nacional de Inteligencia es secreta, reservada, y clasificada, a tal punto que ni la ciudadanía ni ninguna otra autoridad podrán ejercer escrutinio sobre sus actividades, tareas y resultados.

Por ejemplo, en referencia a la adquisición de tecnologías para la vigilancia se llega a afirmar que, en el uso de recursos empleados en su compra, "ninguna autoridad o entidad, podrá detener, interferir, inspeccionar o impedir el traslado de dichos recursos, bajo ninguna circunstancia" (artículo 43). Se trata de una prohibición general incompatible con la transparencia que deben las autoridades en el marco de sus actuaciones públicas.

La LOI prevé dos mínimas excepciones que son insuficientes en términos de contrapesos al poder en manos del SNI. La primera, a través de la cual se concede un muy limitado poder a la Contraloría General del Estado para *conocer*, más no para cuestionar ni pedir información, sobre el uso pasado o actual del "fondo permanente de gastos" del SNI. La Ley Orgánica de Inteligencia incluso llega al extremo de obligar al propio contralor a incinerar la información sobre gastos de la SNI, para asegurar que dicha información no vea la luz de manera alguna (artículo 13).

Y la segunda, que delega a la Comisión Especializada Permanente encargada de la temática de Seguridad, en la Asamblea Legislativa, la facultad de exigir rendición de cuentas a la autoridad encargada del SNI. Esa rendición de cuentas, sin embargo, está condicionada: las solicitudes o requerimientos de los Asambleístas deben estar motivadas y relacionadas únicamente con la fiscalización y control político de la entidad, así como asociadas solo a sus "objetivos, metas e indicadores" (artículo 14).

Es decir, se trata de medidas tan extremadamente limitadas y estrechas en su alcance que obstaculizan cualquier escenario de escrutinio vital en una democracia, y que puedan estar relacionadas no solo con el desempeño y actuación orgánica y operativa del SNI, sino a posibles hechos que involucren actos de corrupción, abusos de poder y de las tecnologías adquiridas, así como violaciones a los derechos humanos.

Según estándares interamericanos en materia de acceso a la información y la transparencia, las autoridades democráticas, incluidas las del sector seguridad y de inteligencia, deben regirse por el principio de máxima divulgación de sus actuaciones, de

modo de “toda la información en poder del Estado se presuma pública y accesible, sometida a un régimen limitado de excepciones”.[101]

Las razones asociadas a la protección de la seguridad nacional para imponer un secreto y una opacidad generalizada resultan incompatibles con el estándar interamericano, que sugiere que las excepciones a la transparencia deben ser únicamente aplicadas en “circunstancias legítimas y estrictamente necesarias en una sociedad democrática”.

La redacción de los artículos 13, 14 y 43 de la LOI no superan el test tripartito de la Convención Americana sobre Derechos Humanos (CADH), artículo 13.2, que fija tres condiciones para justificar las limitaciones legítimas al derecho de acceso a la información: i) estar definidas de forma clara y precisa, ii) estar orientadas al logro de un objetivo legítimo, iii) y estar fijadas en una ley clara y accesible.

En primer lugar, la LOI y su Reglamento hacen de la transparencia una excepción condicionada y en extremo excepcional. La opacidad generalizada, busca la protección abstracta de la protección de la seguridad nacional. Y aunque constan en un marco legal, aquel no se encuentra redactado de “forma acotada y precisa para que las personas comprendan qué información puede ser clasificada, cuál debería ser divulgada y qué actos relativos a la información pueden ser objeto de sanción”,[102] condición necesaria en una sociedad democrática, para el logro de fines imperiosos.

El diseño de las restricciones al derecho al acceso a la información demanda al Estado probar una estricta proporcionalidad de la limitación a la transparencia, y que no se explicita ni muestra en la LOI como medida idónea para lograr un objetivo imperioso. Más aún, la motivación de la LOI cuando fue proyecto careció de toda consideración en ese sentido.

Para lidiar con esta opacidad generalizada, la LOI debió haber aplicado el estándar interamericano en cuestión, apropiando el contenido de los Principios de Tshwane que han sido reconocidos por la Comisión Interamericana de Derechos Humanos (CIDH) como “una buena guía para que los Estados puedan implementar medidas necesarias, cuando se trata de proteger la seguridad nacional en forma consistente con una sociedad

[101] Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos (Julio, 2020). Derecho a la información y seguridad nacional. OEA/Ser,L/V/II, CIDH/RELE/INF.24/20. Disponible en: https://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf ver párrafo 75

[102] Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos (Julio, 2020). Derecho a la información y seguridad nacional. OEA/Ser,L/V/II, CIDH/RELE/INF.24/20. Disponible en: https://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf ver párrafo 84

democrática".[103]

Los Principios de Tshwane, publicados en 2013, consagran obligaciones a los Estados para que divulguen información, aun cuando pueda estar clasificada por motivos de seguridad nacional. Dichos principios reconocen que los Estados deben divulgar de manera proactiva:

- Información sobre las violaciones a los derechos humanos y el derecho internacional humanitario, incluyendo "violaciones sistemáticas o generalizadas de los derechos a la libertad y seguridad personales", que bajo ninguna circunstancia puede ser clasificada (Principios Tshwane, núm. 10, A);

- Información sobre las violaciones a los derechos humanos cometidas bajo regímenes pasados, por lo que el gobierno sucesor debe proteger, preservar y publicar inmediatamente información que se considera de interés público; así como divulgar información de las agencias estatales e individuos que perpetraron dichas violaciones a los derechos (Principios Tshwane, núm. 10, A);

- Información sobre la leyes y reglamentos que justifican la privación de la libertad de las personas, incluida información sobre los métodos de interrogatorio, motivos y cargos sobre detención de personas en contextos de conflicto armado; las circunstancias de muerte de personas fallecidas de las que el Estado es responsable, y la ubicación de sus restos (Principios Tshwane, núm. 10, B);

- Las leyes y reglamentos aplicables a las autoridades militares, de policía, y subunidades de inteligencia, así como sus organismos de supervisión, mecanismos internos de rendición de cuentas y funcionarios a cargo; así como la divulgación de información necesaria para "evaluar y controlar la erogación de fondos públicos, incluidos presupuestos generales, principales rubros e información básica sobre los gastos de tales autoridades (Principios Tshwane, núm. 10, C);

- Información del marco jurídico general en materia de vigilancia, los procedimientos aplicables a su autorización, la selección de objetivos, el uso,

[103] Principios Globales sobre Seguridad Nacional y el Derecho a la Información ("Principios de Tshwane"), (Junio, 2013). Open Society Foundations: Nueva York. Disponible en: https://www.oas.org/es/sla/ddi/docs/acceso_informacion_Taller_Alto_Nivel_Paraguay_2018_documentos_referencia_Principios_Tshwane.pdf

intercambio, almacenamiento y destrucción del material interceptado, incluidas las (i) leyes en materia de vigilancia abierta y encubierta, técnicas de vigilancia como generación de perfiles, minería de datos, etc., (ii) objetivos permisibles en materia de vigilancia, (iii) el umbral de presunción requerido para iniciar o continuar una medida de vigilancia, así como (iv) la duración de medias de vigilancia, (v) los procedimientos para la autorización y revisión de su uso, (vi) los tipos de datos personales que podrán ser recopilados y procesados por motivos de seguridad nacional, y (vii) los criterios aplicables al uso, retención, eliminación y transferencia de dichos datos (Principios Tshwane, núm. 10, E);

- Información sobre las entidades autorizadas a llevar a cabo acciones de vigilancia, las estadísticas de su uso; así como se debe informar a la sociedad sobre cualquier hecho de vigilancia ilegal el cual debe ser público sin que se sacrifique la privacidad de las personas afectadas por dichas actividades (Principios Tshwane, núm. 10, E)

En particular, en cuanto a las obligaciones de transparencia aplicables a la vigilancia de las comunicaciones, el estándar regional está vertido en los "Necesarios y Proporcionados sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones",[104] que también han recibido eco por la Corte IDH en el fallo CAJAR vs. Colombia. En concreto, consagran la publicación de información global de (i) el número de solicitudes de vigilancia a las comunicaciones aprobadas y rechazadas, y (ii) un desglose de solicitudes por proveedor de servicios, autoridad investigadora, el tipo y propósito de la medida, y el número de personas afectadas por cada una, según el tipo de investigación y sus propósitos (Principio 9).

De igual forma, la LOI debió haber explicitado y dado eco de los Principios de Tshwane para la protección y garantía del derecho de acceso a la información más allá de los asuntos dedicados al gasto público en materia de inteligencia, cubriendo asuntos que fueron ignorados también por el Reglamento como (Principios Tshwane, núm. 18 al 25):

- La obligación de considerar solicitudes de acceso a la información, incluso si la información es clasificada;

- La obligación de confirmar o negar por escrito la tenencia o existencia de

[104] Necesarios & Proporcionados, sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones (Mayo, 2014) Electronic Frontier Foundation. Disponibles en: https://necessaryandproportionate.org/es/principios/#los-principios

información clasificada;

- La obligación de expresar por escrito, en un plazo previsto por la ley, los motivos de la negativa de la decisión de entrega de información clasificada, la relación de los motivos de la clasificación, las autoridades o funcionarios que dispusieron dicha clasificación de la información, y los mecanismos legales para la impugnación de dicha negativa;

- La obligación de recuperar o reconstruir la información faltante cuando una autoridad pública no pueda localizar o responder una solicitud de acceso a la información por ausencia, destrucción o imposibilidad de trazabilidad o rastreo de la información en cuestión;

- La obligación de divulgación parcial de partes de documentos o registros, en especial cuando en un documento conste al tiempo información clasificada y no clasificada;

- La obligación a cargo de las autoridades de identificar información con el mayor nivel de precisión posible la información reservada cuya difusión se deniega;

- La obligación de proporcionar información en formatos accesibles;

- El derecho a recurrir las decisiones relativas a la clasificación de la información en un recurso rápido, de bajo costo, ante una autoridad independiente que garantice que dicha revisión será efectiva, y a que la decisión de la autoridad competente sea justificada, fundada y pública.

Así las cosas, la LOI en su redacción actual erige un sistema de inteligencia prácticamente inmune al escrutinio democrático, amparado en un secreto generalizado que niega el acceso a información pública bajo el argumento de la seguridad nacional. Al no incorporar los estándares interamericanos ni los Principios de Tshwane, la ley no solo vulnera el derecho de acceso a la información, sino que también facilita escenarios de corrupción, abuso de poder y violaciones a los derechos humanos.

Para remediar esta situación, el Reglamento de la LOI debió haber corregido el rumbo en materia de preservación del secreto como la regla general Sin embargo, su texto no hace tal ajuste, por el contrario consolida el secreto como regla general y reduce la

transparencia a una excepción, sin cabida en el marco de inteligencia y contrainteligencia del Estado.

Por tanto, solicitamos de manera respetuosa a esta honorable Corte Constitucional, que se sirva declarar inconstitucional por inconvencional al artículo 13, 14 y 43 de la LOI en tanto que contravienen los estándares regionales sobre acceso a la información pública y transparencia en asuntos de seguridad nacional.

VIII. CONCLUSIONES

En función de lo expuesto se recomienda que se acepte la acción de inconstitucionalidad planteada en contra de la Ley Orgánica de Inteligencia y su Reglamento expedido a través del Decreto Nº 52 de 2025.

IX. PETICIÓN

Conforme lo establece el artículo 12 de la LOGJCC solicitamos:

- Se acoja el razonamiento técnico/técnico jurídico expuesto en el presente amicus curiae.
- Se nos permita comparecer en la citada audiencia de sustentación del día 01 de Septiembre para exponer a esta honorable Corte los criterios vertidos en el presente *amicus curiae*.

X. NOTIFICACIONES

Solicitamos a esta honorable Corte Constitucional se sirva remitir notificaciones por medio de correo electrónico a juancarlos@derechosdigitales.org, paloma.lara.castro@derechosdigitales.org, y a lucia.camacho@derechosdigitales.org