# En Ecuador se discute una ley de inteligencia incompatible con los derechos humanos

*En la Asamblea Legislativa de Ecuador avanza la discusión del "Proyecto de ley orgánica de inteligencia" que, si bien busca responder a los retos que enfrenta el país en materia de seguridad nacional, propone un articulado que genera preocupación por su nivel de desprotección de los derechos humanos.*

Por Lucía Camacho[i]

El proyecto de ley[ii] crea el Sistema Nacional de Inteligencia (SNI), a cargo de coordinar diversos subsistemas que estarán dedicados a la inteligencia de sectores como el policial, de las fuerzas armadas, de análisis financiero y económico, de la Casa Militar de la presidencia, tributario, aduanero y del ámbito penitenciario.

El proyecto es preocupante pues fue diseñado para concentrar un poder extraordinario en manos de la autoridad a cargo del SNI. Dicha entidad estará habilitada para: requerir a cualquier entidad pública del Estado –e inclusive, al sector privado- la entrega de bases de datos e información considerada de interés, sin que medie oposición posible; usar gastos reservados para la adquisición indiscriminada, secreta y no supervisada de tecnologías para la vigilancia masiva de las comunicaciones; así como operar de manera blindada por el secreto y la naturaleza clasificada de todas sus actividades, tareas y operaciones.

Instamos a que el **proyecto sea rediseñado en consonancia con estándares interamericanos de protección a la transparencia, la privacidad y la rendición de cuentas** para alinear al Sistema Nacional de Inteligencia con los derechos de las personas. La protección de la seguridad nacional del Estado no debe ser una justificación para sacrificar garantías constitucionales, por lo que llamamos la atención a que, en particular, se preste atención a los siguientes problemas presentes en el proyecto en cuestión.

## Urgen medidas de protección a la transparencia

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 actúa en ejercicio de las facultades que pueden injustamente limitar el ejercicio de derechos.

## Los aspectos problemáticos

El proyecto 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 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.

El proyecto 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. El proyecto incluso llega al extremo de obligar al propio contralor a quemar 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.

## Qué sugerimos

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".[iii]

Las razones asociadas a la protección de la seguridad nacional para imponer un secreto general y opacidad generalizadas 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”.

El proyecto de ley no supera, en su redacción actual, el test tripartito fijado por la Convención Americana sobre Derechos Humanos (CADH), artículo 13.2, que fija tres condiciones para justificar limitaciones al derecho de acceso a la información:

> (i) ser definidas de forma precisa y específica en el proyecto de ley, pues la redacción actual formula criterios de opacidad generalizada, haciendo de la transparencia una excepción condicionada y en extremo excepcional;
>
> (ii) estar orientadas al logro de alguno de los objetivos legítimos de la CADH, o sea, no solo la protección de la seguridad nacional a la que se refiere en repetidas ocasiones el proyecto, sino la protección del orden público, la salud o moral públicas;
>
> (iii) la limitación debe ser fijada en una ley “accesible, inequívoca y redactada 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”[iv]; necesaria en una sociedad democrática, para el logro de fines imperiosos, lo que requiere probar una estricta proporcionalidad de la limitación a la transparencia como medida idónea para lograr un objetivo imperioso, sin embargo, la motivación del proyecto de ley carece de toda consideración en ese sentido.

Para lidiar con esta opacidad generalizada, sugerimos además de aplicar el estándar interamericano en cuestión, apropiar el contenido de los Principios de Tshwane[v] 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 democrática”[vi].

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** la:

- 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, 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, sugerimos aplicar los principios "Necesarios y Proporcionados sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones"[vii], confeccionados en 2013 por más de 40 personas expertas, y respaldada a nivel global por más de 400 organizaciones de la sociedad civil, y que prevén como obligación del Estado la publicación de información crítica en materia de vigilancia de las comunicaciones.

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, para alinear la protección de la transparencia y el acceso a la información en el marco del proyecto, instamos a que se cree un capítulo dedicado a la **protección y garantía del derecho de acceso a la información** en el marco del proyecto de ley de inteligencia, que prevea, entre otros (Principios Tshwane, núm. 18 al 25):

- La obligación de considerar solicitudes, incluso si la información es clasificada;
- La obligación de confirmar o negar por escrito la tenencia o existencia de 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.

## Urgen medidas de protección a la privacidad y protección de datos

El proyecto de ley de inteligencia **centraliza en el Servicio Nacional de Inteligencia un poder informativo sin precedentes en Ecuador y en la región.** Su texto habilita a dicha entidad a elevar solicitudes indiscriminadas de información y bases de datos a las entidades públicas y privadas que los administran; a adquirir de manera no supervisada tecnologías (hardware y software) para desplegar actividades de vigilancia masiva de las comunicaciones; y concede facultades abiertas y vagas para la interceptación de las comunicaciones de las personas.

Tal y como reconoció en 2009 el 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 orbitar en torno a los medios y los mecanismos de producción y recopilación de información y datos que por su naturaleza y condición, suele involucrar la recopilación sigilosa, secreta, no advertida ni consentida por su titular, por lo que el Estado puede terminar amasando grandes cantidades de datos personales que, sin las reglas ni medidas adecuadas, pueden derivar en una intrusión o injerencia arbitraria en la privacidad de las personas.[viii]

Se trata de una situación tan potencialmente crítica y capaz de generar fricción entre las actividades de inteligencia y los derechos de las personas, que la Corte Interamericana de Derechos Humanos (CtIDH), en el reciente fallo **CAJAR *vs* Colombia,** ha enfatizado en la necesidad de la delimitar de manera precisa las "exigencias, requisitos y controles" para hacer compatible la recopilación de información, y más precisamente, de datos personales, en el marco de tareas de inteligencia, con la Convención Americana sobre Derechos Humanos.[ix]

Organismos como el Consejo de Derechos Humanos[x], la Relatoría Especial para la Libertad de Expresión de la ONU y la OEA[xi], la Comisión[xii] y la Corte Interamericanas de Derechos Humanos han advertido sobre la importancia de balancear los intereses de protección a la seguridad nacional con la protección de derechos, así como reiterado la necesidad de reconocer que los **poderes de los servicios de inteligencia en materia de vigilancia de las comunicaciones generan una propensión al abuso**, en especial en la era digital donde el estado del arte tecnológico facilita la recolección intensiva y explotación masiva de información personal de todo tipo.

De ahí la importancia de los mecanismos sustanciales y procedimentales de control y supervisión de estas facultades que sean robustos y estén enfocados en la protección de la privacidad en tanto que éste es un derecho democrático, habilitador e instrumental para otros derechos, como la libertad de expresión, libertad de prensa, derecho a la libre asociación y protesta pacífica, entre otros.

## *Los aspectos problemáticos: tres elementos críticos*

*La solicitud de información en manos de entidades públicas y privadas*

El proyecto de ley crea una arquitectura jurídica que pone a las **entidades públicas y privadas al servicio de la inteligencia estatal**. Crea la obligación de entrega "oportuna", "completa", "segura", "directa" y "gratuita", así como el deber actualización, de la información y bases de datos en manos de dichos actores quienes no podrán oponerse, cuestionar ni alegar excepciones ante las solicitudes de la autoridad encargada del SNI (art. 47, 48, 50, y primera disposición general). Incluso si se tratase de información clasificada en manos de entes públicos, aquellos deberán cumplir con lo pedido por la máxima autoridad de inteligencia.

Esta facultad de alcance masivo y discrecional no tiene contrapeso alguno en el proyecto. El proyecto prevé, sin justificación del trato diferente de la norma, un requisito de motivación debida de la medida solo cuando se dirija dicha orden a los actores del sector público, pero las razones que debe alegar la autoridad responsable del SNI deben apuntar a fines tan amplios como vagos, como la "seguridad integral del Estado" (art. 48).

Además, el proyecto no solo guarda total silencio sobre las condiciones que rigen el intercambio de bases de datos e información entre actores del sistema de inteligencia y otras entidades públicas y privadas; sino que omite por completo cualquier alusión a procesos de intercambio de información entre el sistema de inteligencia ecuatoriano con el de otros países –una actividad natural de los sistemas de inteligencia modernos-.

La deficiencia con que se regula el intercambio de datos e información en el proyecto, aumenta el riesgo inherente de "inclusividad excesiva", un fenómeno descrito por Martín Scheinin como la reunión y recopilación de información tan solo por su utilidad, y no por satisfacer un fin determinado, lo que en última instancia significa el despliegue de un poder de centralización de datos e información que hace de la vigilancia del Estado una práctica cuestionable y problemática.[xiii]

Sobre este punto, la CtIDH en el fallo CAJAR vs Colombia reitera igualmente la importancia de que el intercambio de información entre organismos de inteligencia del Estado o de otros Estados, precise los fines que habilitan a dicho intercambio, las entidades autorizadas y las salvaguardas necesarias para la seguridad y protección de la información, en especial para la protección de datos personales potencialmente cubiertos por dicha medida[xiv].

*La interceptación de las comunicaciones, y los datos de los suscriptores*

El proyecto de ley también obliga a los proveedores de los servicios de telecomunicaciones a entregar un extenso conjunto de información sobre sus usuarios. En ese caso, el proyecto apenas consagra que la orden de entrega de datos debe "debidamente justificada", pero no señala los requisitos que debe satisfacer

dicha motivación, el medio en que debe constar, o las posibilidades, si las hay, para que dichas empresas puedan impugnarla (art. 51).

El SNI, según el proyecto en trámite, puede requerir acceso a la (i) información histórica del abonado celular, (ii) acceso a sus comunicaciones en tiempo real, (iii) información de conexión de los abonados, información técnica, informática, (iv) localización de las celdas donde se encuentran las terminales y, en general, todo tipo de información que facilite la identificación y localización del abonado celular en cuestión (art. 51).

Si bien el artículo 51 dice que se "deberán observar los principios de necesidad y proporcionalidad, evitando en todo momento su aplicación arbitraria", al tiempo, se omite cualquier alusión a cómo serán operacionalizadas en la práctica dichas garantías, por lo que su mención vaga queda vacía de contenido.

Además, prevé que las empresas de telecomunicaciones se encuentran obligadas a almacenar y retener los datos de sus suscriptores y otros datos asociados a las telecomunicaciones por hasta 5 años. Un plazo particularmente extenso comparado con el que rige en países de la Unión Europea donde esa obligación de conservación, por ser altamente invasiva de la privacidad de las personas, se reduce entre los 6 a los 24 meses máximo.

Sobre este asunto, el Relator Especial Martín Scheinin advirtió sobre el riesgo asociado a plazos extensos de retención de datos de los usuarios de los 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.[xv] Al respecto, vale la pena reiterar que, de conformidad al fallo Escher y otros vs Brasil la CtIDH señaló que los metadatos de las comunicaciones también se encuentran protegidos por el derecho a la inviolabilidad de las comunicaciones privadas.[xvi]

Se trata de una distinción que, en palabras del Relator Especial, se encuentra 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.

### *Vigilancia del espectro electromagnético y el ciberespacio*

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

El proyecto no desarrolla con mayor detalle las implicaciones de estas **acciones que articulan tareas de vigilancia del espectro electromagnético y del ciberespacio**, 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.

Sabemos 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. Es, desde luego, **una modalidad más de la vigilancia masiva** que ha sido acusada como tal por organizaciones de la sociedad civil en el contexto colombiano, donde la Ley de Inteligencia prevé el monitoreo del espectro en manos de las autoridades de inteligencia, y que por su naturaleza tiene implicaciones para la privacidad similares a los de la interceptación de las comunicaciones.[xvii]

Se le llama también “pesca milagrosa”, porque si bien no se enfoca en interceptar las comunicaciones de alguien identificado o identificable, y que representa una amenaza concreta para “la soberanía y la seguridad del Estado”, su uso busca identificar si entre cientos o miles de comunicaciones legítimas y privadas surge o no alguna amenaza que llame la atención de las autoridades. De manera que, por sus características, la vigilancia indiscriminada del espectro termina sacrificando de manera arbitraria la privacidad de las personas que nada tienen que ver 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[xviii] por otras autoridades de inteligencia de la región[xix].

La documentación del 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 linea son de supuesto libre uso y acceso por el mero hecho de su publicación. Desde luego, el proyecto 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.

## *Qué sugerimos*

**En primer lugar, sugerimos regular con mucho mayor detalle, precisión y claridad el uso de técnicas y medios aplicables a la recogida, intercambio y almacenamiento de información de inteligencia.**

El Relator Especial Martín Scheinin sugiere en su informe de julio de 2009 la necesidad de que las técnicas y métodos especiales de investigación autorizados para uso de las autoridades de inteligencia deban estar consagradas en la ley a través de disposiciones "sumamente detalladas".[xx]

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 los usuarios de servicios de telecomunicaciones, y el uso de otras técnicas y tecnologías para la vigilancia del espectro electromagnético y el ciberespacio –entre otras-, deben constar en regulaciones específicas y exhaustivas que definan competencias y atribuciones de las autoridades del sistema de inteligencia.[xxi]

En el mismo tenor, la CtIDH en 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" (i) los tipos y medidas, así como acciones de obtención y recopilación de información autorizadas en materia de inteligencia, (ii) los objetivos perseguidos a través de dichas medidas, (iii) 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; (iv) el grado o el umbral de sospecha que puede justificar la recopilación y obtención de la información, (v) los plazos aplicables a las tareas de recolección de información y uso de las técnicas y medios empleados, (vi) y los métodos útiles para actualizar, supervisar, examinar, obtener y recopilar dicha información.[xxii]

El Relator M. 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. 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".[xxiii]

**En segundo lugar, recomendamos que el proyecto de ley de inteligencia en cuestión, esté alineado con la protección de datos como un derecho que también resulta aplicable a las tareas de inteligencia, tal y como fue reconocido explícitamente en el fallo CAJAR vs Colombia.**

Para ello, la CtIDH sugirió que, cuando la recopilación y almacenamiento de información de inteligencia involucre el procesamiento de datos personales, se deben crear disposiciones para crear políticas de protección de datos que permitan mantener registros que (i) identifiquen a los responsables de la información recopilada, (ii) se describan 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 éstos.[xxiv]

Las reglas que orienten la protección de datos aplicables a las tareas de inteligencia, deben estar proyectadas no solo relación con el tratamiento de datos contenidos en la "información accionable" de inteligencia, sino también cuando éstos empiezan a ser parte de los archivos de inteligencia sobre los cuales la CtIDH, en el caso CAJAR vs Colombia, reconoció expresamente el derecho que tienen los titulares de los datos a ejercer el derecho a la cancelación, actualización o eliminación de los mismos[xxv]. El proyecto de ley de Ecuador debe abordar seriamente también esta materia.

Llamamos la atención para que el proyecto regule sobre estas materias pues la reciente Ley Orgánica de Protección de Datos aprobada en 2021, no aplica para las tareas de inteligencia, más aún, dicha ley prevé la creación de reglas en materia de protección de datos para la seguridad nacional deban, 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"[xxvi] (artículo 11).

**En tercer lugar, recomendamos que las medias más invasivas de la privacidad de las personas, estén sujetas a mecanismos de revisión judicial, consten en una orden escrita, y estén debidamente motivadas.**

Para el Relator Martín Scheinin[xxvii], así como para la CtIDH en el caso CAJAR vs Colombia[xxviii], existe la necesidad de que las medidas y tecnologías más invasivas a la privacidad sean objeto de revisión independiente de una autoridad judicial. Los Principios Necesarios y Proporcionados, también coinciden en este punto (ver principio 6).

A esta autorización debe someterse el uso de técnicas invasivas abiertas o encubiertas de inteligencia[xxix], la vigilancia e interceptación de las comunicaciones análogas y digitales[xxx], y hasta el uso de programas espías para controlar de manera remota los dispositivos digitales.[xxxi]

Reconocemos que el derecho a la privacidad no es absoluto y puede ser limitado de manera compatible con la CADH siempre que sean satisfechos los requisitos de legalidad, realización de un fin legítimo, y cumplimiento de los requisitos de idoneidad, necesidad y proporcionalidad.

Pero, en línea con lo reconocido por la CtIDH en el caso CAJAR vs Colombia, no ignoramos que el estado del arte tecnológico así como la continua diversificación y sofisticación de las técnicas y tecnologías que facilitan la recopilación y obtención de información de inteligencia de manera "selectiva o a gran escala", aumentan de manera extrema el riesgo de abuso y arbitrariedad en el uso de estas facultades en manos de las autoridades de inteligencia. Por lo que una autoridad judicial debe

decidir sobre la procedencia de estas medidas, y que debe decidir sobre los límites en materia de modo, tiempo, duración y alcance de la medida autorizada.[xxxii]

Por tanto, las ordenes a las que refiere en proyecto de ley que afectan potencialmente la privacidad de las personas, deben constar por escrito, y estar debidamente justificadas en una causa probable o motivos fundados, que relacionen al tiempo fundamentos de hecho y la satisfacción del umbral de sospecha previsto en la ley que sea aprobada.[xxxiii,xxxiv]

**Y en cuarto lugar, recomendamos que el contenido del proyecto de ley refleje las buenas prácticas aplicables en derechos humanos a las tareas de inteligencia y seguridad nacional, diseñadas por el Relator Especial Martín Scheinin, y de las cuales hace eco la CtIDH en el fallo CAJAR vs Colombia.**

Entre las buenas prácticas, se identifica la adopción de los siguientes principios[xxxv]:

- Principio de intrusión mínima: Toda decisión de crear una nueva base de datos, intercambiar información o ejecutar medidas intensivas de vigilancia se deben basar en una necesidad demostrada.
- Principio de especificación del fin para limitar las utilizaciones secundarias: Los Estados deben crear una base legal para la reutilización de información de inteligencia de acuerdo con los principios de derechos humanos, en especial cuando sea intercambiada entre Estados y autoridades que recopilaron información para otros fines y la entregar a las autoridades de inteligencia.
- Principio de supervisión y autorización regulada: los organismos de inteligencia precisan de mecanismos independientes de salvaguardias para la prevención e investigación de posibles abusos. La práctica de “auto-autorización” de tareas y órdenes de inteligencia, en tanto que propensa al abuso, debe ser reemplazada por mecanismos de autorización independiente.
- Principio de transparencia e integridad: Este principio entraña los deberes de notificar a la persona afectada por actividades de vigilancia “tan pronto como sea posible inmediatamente después”[xxxvi] de ejecutada la medida de vigilancia en cuestión pues “la falta de limitaciones claras y adecuadas de la política de vigilancia hace difícil demostrar que esos poderes no se utilizan de manera arbitraria e indiscriminada”.[xxxvii]
- Principio de modernización efectiva: en razón a la modernización y sofisticación continua y progresiva de las tecnologías de vigilancia de las comunicaciones, los Estados deben adoptar medidas de evaluación de impacto a la privacidad, lo que permitiría afianzar una cultura de la privacidad en organismos de gobierno que despliegan ese tipo de tareas.

Asimismo, sugerimos incluir en el proyecto de ley mecanismos de reparación de derechos en los casos en que se haya abusado de las facultades, medios o técnicas de

vigilancia empleados y se haya concretado una situación de intrusión arbitraria o ilegal de la privacidad de las personas (principio 13, de los principios “Necesarios y Proporcionados). Dicho mecanismo de reparación debe ser efectivo, e incluir también vías de protección a los alertadores (o *whistleblowers*) que informan de dichos abusos y permiten transparentar las actuaciones ilegales de las autoridades ante la ciudadanía.

## Conclusiones

El diseño de sistemas de inteligencia completamente opacos, blindados por el secreto y la clasificación total de sus actividades y operaciones, son incompatibles con estándares de derechos humanos y no deben tener cabida en los sistemas democráticos.

El proyecto de ley en Ecuador fue diseñado a partir de una visión en extremo canónica de las actividades de inteligencia donde la transparencia, la privacidad ni la protección de datos de la población tienen cabida. De ser aprobada, la ley de inteligencia sería abiertamente inconstitucional e inconvencional.

Extendemos un llamado a las organizaciones de la sociedad civil para intensificar el escrutinio del proyecto de ley en cuestión; así como hacemos un llamado de atención a las autoridades de la Asamblea Legislativa de Ecuador para rediseñar el proyecto de ley de inteligencia para que, desde su concepción, está alineada a los derechos humanos y sea fruto de la participación significativa de la sociedad civil interesada.

Y finalmente, en caso de que el proyecto no sea susceptible de modificación, instamos a su total rechazo en tanto sería no solo abiertamente inconstitucional sino contrario a compromisos internacionales del Estado. De seguir adelante con la propuesta legislativa, recomendamos firmemente rediseñar su contenido en consonancia con estándares interamericanos de protección a la transparencia, la privacidad y la rendición de cuentas para alinear al Sistema Nacional de Inteligencia con los derechos de las personas.

i Coordinadora de políticas públicas. Contacto lucia.camacho@derechosidigitales.org

ii Asamblea Nacional (Junio, 2025). Pleno de la Asamblea Nacional tramitó en segundo debate el proyecto de leyt orgánica de inteligencia. Disponible en: https://www.asambleanacional.gob.ec/es/noticia/106626-pleno-de-la-asamblea-nacional-tramito-en-segundo-debate

iii 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

iv 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

v 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

vi 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 86

vii 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

viii 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, Martín Scheinin, A/HRC/10/3, del 4 de febrero de 2009. Disponible en: https://digitallibrary.un.org/record/648291/files/A_HRC_10_3-ES.pdf párrafos 26 y siguientes

ix 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. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf párrafo 520 y 527

x 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.

xi 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.

xii 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

xiii 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, Martín Scheinin, A/HRC/10/3, del 4 de febrero de 2009. Disponible en: https://digitallibrary.un.org/record/648291/files/A_HRC_10_3-ES.pdf párrafo 32 y siguiente

xiv 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. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf párrafo 539

xv 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, Martín Scheinin, A/HRC/13/37, del 28 de diciembre de 2009. Disponible en: https://www.refworld.org/es/ref/infortem/cdhonu/2009/es/72748 párrafo 42 y siguientes

xvi Corte Interamericana de Derechos Humanos, Caso Escher y otros vs Brasil, Sentencia del 6 de julio de 2009. Excepciones preliminares, fondo, reparaciones y costas. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf párrafo 114 y siguientes

xvii 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

xviii 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/

xix 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

xx 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, Martín Scheinin, A/HRC/10/3, del 4 de febrero de 2009. Disponible en: https://digitallibrary.un.org/record/648291/files/A_HRC_10_3-ES.pdf párrafos 27 y siguientes

[xxi] 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, Martín Scheinin, A/HRC/10/3, del 4 de febrero de 2009. Disponible en: https://digitallibrary.un.org/record/648291/files/A_HRC_10_3-ES.pdf párrafos 27 y siguientes

[xxii] 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. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf párrafo 538

[xxiii] rotección de los Derechos Humanos y las Libertades Fundamentales en la Lucha Contra el Terrorismo, Martín Scheinin, A/HRC/10/3, del 4 de febrero de 2009. Disponible en: https://digitallibrary.un.org/record/648291/files/A_HRC_10_3-ES.pdf párrafo 31

[xxiv] 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. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf párrafo 540

[xxv] 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/24094/historica-sentencia-de-la-corte-interamericana-de-derechos-humanos-la-proteccion-de-datos-aplica-en-las-tareas-de-inteligencia/

[xxvi] Ley Orgánica de Protección de Datos Personales (2021). Asamblea Nacional, Presidencia de la República de Ecuador. Disponible en: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

[xxvii] 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, Martín Scheinin, A/HRC/10/3, del 4 de febrero de 2009. Disponible en: https://digitallibrary.un.org/record/648291/files/A_HRC_10_3-ES.pdf párrafo 29

[xxviii] 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. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf párrafo 542

[xxix] 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, Martín Scheinin, A/HRC/13/37, del 28 de diciembre de 2009. Disponible en: https://www.refworld.org/es/ref/infortem/cdhonu/2009/es/72748 párrafo 21

[xxx] 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. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf párrafo 542

[xxxi] 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, Martín Scheinin, A/HRC/13/37, del 28 de diciembre de 2009. Disponible en: https://www.refworld.org/es/ref/infortem/cdhonu/2009/es/72748 párrafo 21

[xxxii] 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. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf párrafo 547

[xxxiii] 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, Martín Scheinin, A/HRC/10/3, del 4 de febrero de 2009. Disponible en: https://digitallibrary.un.org/record/648291/files/A_HRC_10_3-ES.pdf párrafo 30

[xxxiv] 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. Disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf párrafo 547

[xxxv] 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, Martín Scheinin, A/HRC/13/37, del 28 de diciembre de 2009. Disponible en: https://www.refworld.org/es/ref/infortem/cdhonu/2009/es/72748

[xxxvi] 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, Martín Scheinin, A/HRC/13/37, del 28 de diciembre de 2009. Disponible en: https://www.refworld.org/es/ref/infortem/cdhonu/2009/es/72748 párrafo 55

[xxxvii] 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, Martín Scheinin, A/HRC/13/37, del 28 de diciembre de 2009. Disponible en: https://www.refworld.org/es/ref/infortem/cdhonu/2009/es/72748 párrafo 54