Aporte conjunto a la 'Convocatoria de Aportaciones sobre los Impactos en los Derechos Humanos del Uso de la Inteligencia Artificial en la Lucha contra el Terrorismo', de la Relatoría Especial sobre la lucha contra el terrorismo y los derechos humanos

Agosto 29, 2025

Resumen

Este aporte llama la atención de esta Relatoría para que se aproxime la IA en razón a sus capacidades, arquitectura y diseño, no se trata de una tecnología homogénea con impactos predecibles. La IA con capacidades predictivas debe ser abordada con mucha mayor precaución y se debe llamar a la prohibición de su uso para tareas de lucha contra el terrorismo.

En América Latina delimitamos el estado de esta intersección bajo tres perspectivas. La primera, la réplica de la regulación de la IA en Europa que habilitará en la región el uso de tecnologías de identificación biométrica remota también para la lucha contra el terrorismo, con los riesgos que esto acarrera para el espacio cívico, incluida la protección de la privacidad. La segunda, la amenaza de potencial uso dual de tecnologías que ya se encuentran desplegadas en la región, como el reconocimiento facial para la seguridad ciudadana. Y en tercer lugar, identificamos una nueva oleada de reformas regulatorias en lucha contra el terrorismo que habilitan y dan luz verde al uso de cualquier tecnología en dicho terreno. Concluimos con recomendaciones para esta Relatoría y el diseño de su informe enfocado en esta materia.

Introducción: Uso estatal de la IA para tareas de antiterrorismo en América Latina

La consulta sobre la cuestión de los impactos en derechos humanos del uso de inteligencia artificial en la lucha contra el terrorismo llega en un momento crucial para América Latina. La región se encuentra en la encrucijada entre dos procesos preocupantes:

1) La creciente incorporación de tecnologías genéricamente descritas como "inteligencia artificial" por parte de los gobiernos para distintas funciones, pero especialmente para tareas de vigilancia e inteligencia. Esta incorporación se realiza en casi todos los casos sin discusiones previas sobre su impacto en derechos humanos, sin mediar estudios de su impacto, sin informar las características y arquitectura de las tecnologías en cuestión, sin transparencia sobre sus potencialidades y riesgos ni de las empresas fabricantes de dichas tecnología, y sin establecer mecanismos de monitoreo y rendición de cuentas adecuados.

2) El uso cada vez más frecuente de la narrativa de lucha contra terrorismo como forma de encuadrar diversos fenómenos de procesos políticos y/o criminales que poco o nada tienen que ver con éste, desde la criminalidad organizada hasta la persecución de la disidencia política. Muchos gobiernos regionales se apoyan en el hecho de que en las últimas décadas se naturalizó que la cuestión del "antiterrorismo" admite niveles de secreto y discrecionalidad excepcionales, permitiéndoles usarlo como coartada para evitar controles y procedimientos acordes a las garantías básicas de un Estado democrático.

La intersección entre estos dos procesos produce una situación de opacidad agregada o aumentada: al secreto que rodea todo lo relacionado con las medidas y políticas antiterroristas, se suma el secreto comercial que esgrimen las empresas productoras de tecnologías digitales –como la IA, la biometría, el reconocimiento facial, entre otros– para negarse a informar las condiciones de funcionamiento y posibles riesgos que acarrean sus productos.

Desde el punto de vista de la sociedad civil resulta difícil contestar muchas de las preguntas planteadas por la relatoría en su consulta porque las condiciones reales en las que desarrollamos nuestro activismo son de escaso o nulo acceso a información de parte del Estado y las empresas.

Nuestro punto de partida en este informe, que apunta a posicionar el estado de la cuestión sobre despliegue de tecnologías digitales en la lucha contra el terrorismo, es el **llamado a una moratoria indefinida** en la incorporación de las tecnologías genéricamente caracterizadas como "de inteligencia artificial" en dicha materia, hasta tanto se (i) modifiquen estas condiciones de máxima opacidad y secreto en su adopción, y (ii) se robustezcan desde una perspectiva de derechos humanos los marcos legislativos asociados a la lucha contra el terrorismo (como los de inteligencia y vigilancia de las comunicaciones, de persecución penal, entre otros). Y que en dicha moratoria se identifiquen usos y tecnologías –en especial, las de carácter predictivo– cuya apropiación y despliegue, por sus riesgos significativos, pueden desviar los esfuerzos en la lucha contra el terrorismo para fines

antidemocráticos e incompatibles con los derechos humanos, **por lo que deben estar prohibidos**[1].

Para abordar algunas de las preocupaciones y tendencias que observamos en diversos países de la región, en este informe aproximamos en primer lugar los tipos de IA que por sus características representan un más elevado riesgo para la lucha contra el terrorismo; en segundo lugar, enfocamos la atención en tres tendencias regionales observadas y de interés para la convocatoria de esta Relatoría; y en último lugar se sugieren recomendaciones para la Relatoría en la elaboración de su informe.

1. Urge abordar los impactos diferenciados de la IA en tareas antiterrorismo: IA generativa e IA predictiva

La Relatoría hace un uso amplio de la expresión "inteligencia artificial" en el marco de su más reciente consulta[2], sin embargo, el concepto de IA es un término paraguas para un conjunto disímil de tecnologías. Por ejemplo, ChatGPT tiene muy poco en común con los sistemas que utilizan los bancos para evaluar riesgo crediticio. Ambas son aplicaciones de IA, pero en todas las formas sustantivas, son diferentes.[3]

Podemos establecer dos grandes grupos de tecnologías dentro del amplio paraguas de la Inteligencia Artificial, **las IAs generativas y las IAs predictivas.**

Los artefactos de lenguaje natural, los generadores de imágenes, videos y música que asombraron al mundo en los últimos meses forman parte del conjunto de sistemas generativos. Se trata de productos que ya están al alcance de la mano de millones de usuarios a costos deliberadamente bajos, pero que todavía son inmaduros y cuya popularización ha sido acompañada por un amplio espectro de reacciones, desde entusiasmo ciego hasta pánico por sus usos en desinformación, estafas o su impacto en el trabajo.

A. La IA predictiva aplicada a tareas anti-terrorismo supone riesgos más elevados para los DDHH

En contraste, los sistemas de IA predictivos son aquellos que hacen predicciones sobre el futuro para guiar la toma de decisiones en el presente. Estos sistemas ya se están usando tanto en el sector público como en el privado, pero esto no significa que funcionen correctamente. Es muy difícil predecir el futuro, pero es muy fácil confundir ese futuro con una profecía auto confirmatoria basada en patrones estadísticos. El principal problema que advertimos es que la IA predictiva se promociona hoy para **tomar decisiones que impactan sobre el presente y el futuro de las personas**. Este es el campo de **mayor riesgo** para los derechos fundamentales de la ciudadanía.

---

[1] Otras informes de ONU han hecho llamados de este tipo, por ejemplo, recomendando la prohibición de uso de sistemas de IA de alto riesgo (informe A/HRC/48/31 de 2021); la prohibición de sistemas de reconocimiento facial en protestas y de uso de sistemas de vigilancia masiva e indiscriminada (A/HRC/44/24 de 2020).
[2] Call for Input – Position Paper on the Human Rights Impacts of Using Artificial Intelligence in Countering Terrorism. En: https://www.ohchr.org/en/calls-for-input/2025/call-input-position-paper-human-rights-impacts-using-artificial-intelligence
[3] Narayanan, A.; Kapoor, S. (2024). AI Snake Oil: What artificial intelligence can do, what it can't, and how to tell the difference. Princeton University Press.

Así, consideramos necesario, también, precisar el uso del concepto de "IA" por parte de la comunidad y de los organismos internacionales, con el objeto de poder brindar aportes más precisos y efectivos. Sugerimos ajustar las preguntas formuladas por la Relatoría Especial en este sentido, para así afinar nuestras respuestas. A modo de ejemplo, podemos mencionar las definiciones de la Unión Europea (UE) y de la Organización para la Cooperación y el Desarrollo Económicos (OCDE).

La primera, en el **la Ley de IA,** define a esa tecnología como "*un sistema basado en máquinas que está diseñado para funcionar con diversos niveles de autonomía y que puede mostrar capacidad de adaptación tras su despliegue, y que, para objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales*"[4] (art. 3).

Por su parte, la **OCDE** la define como "*Un sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere, a partir de la información que recibe (input), cómo generar resultados como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los distintos sistemas de IA varían en sus niveles de autonomía y adaptabilidad tras su despliegue*"[5].

Como podemos observar, ambas definiciones se basan en el proceso de inferencia que realizan las máquinas, ya sea para generar alguna clase de información o para predecir hechos (fenómenos, conductas, etc). La falta de distinción hecha en la consulta de esta Relatoría en relación al tipo de implementación de **IA sobre la cual se emite una consideración es problemática**, porque el rango de calidad en el funcionamiento y de potencial daño de los diferentes sistemas es tan grande que complejiza la utilización de ese término en la evaluación de impacto sobre DDHH. Es por eso que **recomendamos establecer una mirada de mayor precisión** a la hora de realizar evaluaciones de impacto.

En concreto, cuando hablamos de **IA predictiva** nos referimos, como su nombre lo indica, al cálculo de posibilidades de hechos futuros en función de datos o información existente con los que se alimenta al sistema. Es decir que no se desprende de la mera observación o recolección de información, sino que implica una operación de inferencia sobre ella[6]. Tampoco se trata de una "deducción" o un proceso lógico mediante al que se arribe al resultado con absoluta certeza. Por el contrario, no es más que un cálculo estadístico que

[4] Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, del 13 de junio de 2024, por el que se establecen normas armonizadas sobre inteligencia artificial y se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Ley de Inteligencia Artificial). En: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:L_202401689

[5] OECD (2023). The State of Implementation of the OECD AI principles four years on. OECD Artificial Intelligence Papers, N° 3. En: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/10/the-state-of-implementation-of-the-oecd-ai-principles-four-years-on_b9f13b5c/835641c9-en.pdf

[6] Fundación Vía Libre (2023). Protección legal de datos personales inferidos. En: https://www.vialibre.org.ar/wp-content/uploads/2023/07/ViaLibre2023_Proteccion-legal-datos-personales-inferidos_versionliviana.pdf

arroja resultados probabilísticos, y por lo tanto falibles, especialmente cuando hablamos de conductas y características humanas[7].

A pesar de tratarse de un estudio de probabilidades, es este tipo de IA el que se utiliza generalmente para **el diseño, el monitoreo y la toma de decisiones en políticas públicas y, más especialmente, de seguridad.** Nos referimos, por caso, a los sistemas de *scoring* o puntaje para prever conductas delictivas, o los controles diferenciales en aeropuertos derivados de alertas emitidas por estos sistemas. En ambos casos, se presume la mayor posibilidad de una conducta penada por la ley en función de la pertenencia a ciertos grupos.

Dicho de otro modo, se proyectan sobre individuos tendencias asociadas a colectivos, que a su vez pueden tener distinto grado de verosimilitud. Pensemos por ejemplo en la asociación entre pertenencia a la religión musulmana y terrorismo, a ciertas zonas geográficas y los delitos contra la propiedad, etc. El resultado de estas asociaciones y **procesos de inferencia es un grado alto de discriminación**, que se vuelve más preocupante cuando hay derechos básicos involucrados. Esto se agrava cuando el proceso por el que se arribó al resultado o "alerta" que lleva a tomar la decisión discriminatoria no puede ser explicado (y por lo tanto adecuadamente discutido y ajustado a derecho), por falta de transparencia algorítmica y/o secreto comercial alegado por las empresas a cargo. Finalmente, debemos contemplar también que el resultado ("output") de estos procesos suele utilizarse para alimentar el *dataset* de otro sistema (o del propio), arrastrando errores, acentuando los sesgos y aumentando exponencialmente los riesgos de discriminación.

B. La IA predictiva es incompatible con toma de decisiones basadas en la evidencia para las tareas anti-terrorismo

Así las cosas, el problema no es (sólo) los "errores" que pueden tener los sistemas de IA. Aún cuando funcionan acorde a su diseño, los resultados pueden estar alejados de la realidad y causar severos daños a los derechos humanos. Es que no se puede "predecir" el futuro, y menos aún cuando involucra a personas; es muy fácil confundir predicción con profecía autoconfirmatoria. Tomar decisiones de tan alto impacto basado en estadísticas no debería permitirse: **los sistemas de IA predictiva no deben utilizarse en la lucha contra el terrorismo**, sobre todo teniendo en cuenta el grado de vulnerabilidad que implica para quienes son objeto de esos procesos.

Existen numerosos informes de la propia Relatoría Especial sobre la Lucha contra el Terrorismo y los Derechos Humanos sobre el deber reforzado de protección de derechos humanos en el contexto de la lucha contra el terrorismo, especialmente teniendo en cuenta que muchas veces las actividades que se realizan con este objetivo (de vigilancia, por caso) permanecen en secreto y con débiles mecanismos de control. Tal vez **podría aceptarse su uso en supuestos en los que no estén en juego derechos humanos como consecuencia de los resultados que arroje:** pensamos, a modo de ejemplo, en los sistemas de IA aplicados al análisis del flujo de activos financieros en el marco de

[7] En otras palabras, estos sistemas funcionan siguiendo la lógica de que si la persona P tiene los atributos p1, p2, p3 y p4, existe una cierta probabilidad de que tenga (o no tenga) un cierto atributo "Px" no observado (por ejemplo, la propensión a adquirir ciertos bienes o servicios, o —con consecuencias más graves para la privacidad— que tenga una determinada condición de salud).

investigaciones sobre financiación de actividades de grupos terroristas. Se trata de una circunstancia claramente distinta a si se aplicara al flujo de personas y sus desplazamientos o movimientos migratorios si quedaran sujetos a los cálculos estadísticos realizados sin control ni auditoría por un sistema de IA.

En este sentido, y más allá de insistir en la incompatibilidad de la IA predictiva con la los esfuerzos de lucha contra este fenómeno cuando estén en juego derechos, consideramos necesario hacer hincapié en la instancias de rendición de cuentas para el uso de cualquier tipo de tecnología en estos contextos, y la urgencia de reforzarlas.

C. La IA no es auditable, por tanto no debería ser usada en tareas anti-terrorismo

Es importante notar que muchas de las legislaciones que existen hoy en distintas áreas terminan por ser un obstáculo para el correcto monitoreo y medición de su desempeño y funcionamiento. Nos referimos tanto al secreto en temas de seguridad nacional, que suele funcionar como paraguas para evitar dar información pública, como al secreto comercial y las leyes de propiedad intelectual.

En este sentido nos encontramos con los Tratados Internacionales de la Organización Mundial para la Propiedad Intelectual, OMPI, y las legislaciones que los operativizan, como el Digital Millennium Copyright Act (1996) de Estados Unidos, que **impiden realizar procesos de ingeniería reversa sobre software**. Podemos pensar también en casos regionales, como el caso judicial por el uso de Tecnología de Reconocimiento Facial en la Ciudad Autónoma de Buenos Aires (Argentina) para la identificación y detección de prófugos, donde el Gobierno no cumplió con la orden judicial de cumplir con la auditoría exigida judicialmente porque la empresa desarrolladora no entregó la información correspondiente amparada en razones de protección a su propiedad intelectual.

En otro caso sobre cómo la propiedad intelectual es una razón que inhibe la transparencia de las tecnologías en manos de los Estados tuvo lugar en Colombia, e involucró a la aplicación oficial para el rastreo digital de contactos en la pandemia, CoronApp. En dicho escenario, la Agencia Nacional Digital obstaculizó el acceso al código fuente de la aplicación cuyas características querían ser auditadas por la ciudadanía.

Las razones para inhibir la entrega de información pública se apoyaron en la protección a la propiedad intelectual[8], siendo descartadas por la Corte Constitucional en una acción de amparo que tomó cuatro años en ser decidida. La Corte descartó dicha motivación por no estar contemplada en el marco legal de acceso a la información pública de Colombia como una motivación válida para que las autoridades justificasen la retención de información pública.[9]

[8] Lucía Camacho (La Sillva Vacía, Marzo 22 de 2025). CoronApp: datos públicos y la lección que deja la Corte. En: https://www.lasillavacia.com/red-de-expertos/red-de-democracia-y-tecnologia/coronapp-datos-publicos-y-la-leccion-que-deja-la-corte/

[9] Corte Constitucional de Colombia, sentencia T-067/2025, Magistrado Ponente: Natalia Angel Cabo. En: https://www.corteconstitucional.gov.co/relatoria/2025/t-067-25.htm

2. Tendencias regionales

En nuestro trabajo regional advertimos que la relación entre la adopción de la IA –y sus diversas modalidades- en la lucha contra el terrorismo todavía no se perfila por ahora como una prioridad de los tomadores de políticas públicas, sin embargo, identificamos algunas tendencias que permiten advertir cómo la adopción de tecnologías digitales en el marco de la seguridad ciudadana, así como esfuerzos de regulación para la IA, pueden eventualmente apuntar hacia dicho objetivo de manera poco clara y transparente.

En ese sentido, advertimos **tres tendencias regionales** relevantes para la consulta de esta Relatoría:

- Las regulaciones sobre la IA habilitarían al uso de sistemas de IA de alto riesgo, los sistemas de biometría a distancia, tanto en tiempo real como retrospectiva, para la lucha contra delitos graves, incluida la lucha contra el terrorismo
- En países de América Latina, existe el riesgo de uso dual de los sistemas de reconocimiento facial desplegados para la seguridad ciudadana, para ser usados en la lucha contra el terrorismo
- Hay también una nueva oleada regulatoria de los marcos de inteligencia y contra-terrorismo que erosionan garantías previas, y habilitan al uso indiscriminado de tecnologías digitales, incluida la IA.

A. Las regulaciones sobre la IA habilitan al uso de la biometría a distancia –en tiempo real, y retrospectiva- en la lucha contra el terrorismo

Entre los años 2024 a 2025 se ha impulsado en los Congresos o Asambleas Legislativas de varios países en América Latina más de 200 proyectos de ley[10] que buscan establecer regímenes generales de regulación de la inteligencia artificial, o que modifican la arquitectura jurídica preexistente en materia de consumo, protección de datos, el código penal, entre otros, para actualizar su contenido a los retos que trae consigo dicha tecnología.

La biometría en tiempo real y a distancia

Las iniciativas legislativas que buscan establecer regímenes generales de regulación de la IA, imitan o reproducen en buena medida el enfoque de riesgos de la Ley Europea de la Inteligencia Artificial que autoriza el uso excepcional de sistemas de **IA de alto riesgo** como la **identificación biométrica a distancia y en tiempo real** para tareas de lucha contra ciertos delitos, incluida la lucha contra el terrorismo.[11]

Algunas iniciativas regionales, de hecho, **abordan de manera extremadamente vaga la utilización excepcional de este tipo de sistemas de IA de alto riesgo** para tareas de prevención de amenazas inminentes o riesgos para la seguridad, lo que podría abrir la puerta

[10] Mapeo propio de Derechos Digitales desde 2024 y actualizado hasta el 31 de julio de 2025.
[11] Ley de IA en Europa, artículo 5, apartado 1, párrafo primero, letra h), inciso iii)

para su uso para fines de lucha contra el terrorismo. Esta vaguedad resulta crítica en países de América Latina con un largo historial de abuso de tecnologías de vigilancia[12] para la represión de la libertad de expresión, el derecho a la protesta, libre asociación, el derecho a defender derechos, entre otros, y supone un riesgo para garantías fundamentales como el debido proceso y el principio de legalidad.

En distintos países de la región se tramitan proyectos de ley que hacen eco de la regulación europea y habilitan el uso de esta tecnología para tareas asociadas a la lucha contra **amenazas graves o inminentes para la seguridad,** y que son expresiones suficientemente vagas para comprender cualquier tipo de acción estatal. En cada iniciativa en cuestión, los sistemas de IA de biometría remota son calificados de alto riesgo o sinónimos como el "riesgo crítico" o "excesivo", que lo son por su grave impacto para los derechos fundamentales. Entre los proyectos de ley en trámite se encuentran:

- **Colombia**, proyecto de ley N° 043 de 2025[13]: El proyecto es de iniciativa del gobierno, y señala que los **sistemas de IA de "riesgo crítico"** son aquellos cuyo desarrollo o utilización puede ir en contra de los derechos fundamentales, la dignidad humana o el interés público superior, podrían ser empleados excepcionalmente bajo condiciones de trazabilidad, control, evaluación de su impacto y una finalidad legítima previamente definida.

  Entre los tipos de IA de "riesgo crítico" se habilitaría al uso de **sistemas de biometría remota en tiempo real** cuando "exista autorización judicial específica y motivada, y se trate de casos de interés público urgente, tales como (sic) búsqueda de personas desaparecidas, prevención de amenazas inminentes o persecución de delitos graves conforme al ordenamiento jurídico" (Artículo 5, numeral 1, literal c).

- **Chile**, proyecto de ley N° 16821-19 de 2024[14]: El proyecto de ley, de iniciativa del gobierno, prevé el uso excepcional de **sistemas de IA de riesgo inaceptable**, como la **identificación biométrica remota en tiempo real** en espacios de acceso público por las "autoridades y órganos encargados de la seguridad pública y organismos de persecución penal, con el objetivo de prevenir, investigar, detectar y, eventualmente, ejecutar sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública" (Artículo 6, numeral 2, literal e).

[12] Entre los hitos judiciales que ponen de relevancia esta situación se encuentra el fallo Cajar vs. Colombia emitido en 2024 por la Corte Interamericana de Derechos Humanos, sobre abuso del sistema estatal de inteligencia y el uso de tecnologías digitales que facilitan actividades de vigilancia masiva sobre las personas y sus comunicaciones.
[13]Congreso de Colombia, Proyecto de Ley N° 043/2025 "Por medio de la cual se regula la inteligencia artificial en Colombia para garantizar su desarrollo ético, responsable, competitivo e innovador y se dictan otras disposiciones". En: https://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2025%20-%202026/PL%20043-25%20-%20REGULACION%20INTELIGENCIA%20ARTIFICIAL.pdf
[14] Congreso de Chile, Boletín n. 16821-19 "Que formula indicaciones al proyecto de ley que regula los sistemas de Inteligencia Artificial". En: https://www.camara.cl/verDoc.aspx?prmID=34551&prmTIPO=OFICIOPLEY
*refundido con el proyecto de ley N° 15869-19

- **Brasil**, proyecto de ley 2338 de 2023[15]: El proyecto de ley prevé el uso excepcional de **sistemas de IA de riesgo excesivo**, como la **identificación biométrica a distancia y en tiempo real**, para fines como la investigación criminal, circunstancias que signifiquen una amenaza grave e inminente para la vida o integridad de las personas, situaciones en las que se debe atender de manera proporcional y estricta el interés publico, el debido proceso y el control judicial, especialmente la garantía de no discriminación y la revisión de la inferencia algorítmica por la autoridad responsable (Artículo 13, numeral IV, literal a-d).

En el caso de Brasil y de Chile, donde las discusiones legislativas se encuentran más avanzadas, se encuentran actualmente desplegados sistemas de reconocimiento facial –una de las modalidades más comunes de biometría remota– cuya despliegue puede ser explotado también para fines de lucha contra el terrorismo –tal y como veremos en las secciones siguientes–.

La biometría remota y retrospectiva o ulterior

Estos mismos países habilitarían, al igual que lo hace la Ley de IA en Europa, al uso de **sistemas de biometría remota retrospectiva o ulterior** –calificada también como de Alto Riesgo–, es decir, otro tipo de biometría remota que tiene lugar sobre grabaciones pasadas, y que incentiva a una mayor retención de imágenes y videos para habilitar a la identificación de las personas que aparecen en una imagen o video.[16]

De hecho, estas propuestas reproducen el mismo enfoque regulatorio vigente en Europa, que autoriza de manera excepcional el uso de la biometría remota en tiempo real para supuestos de gravedad, y la autorización sin mayores condiciones en el uso de sistema de biometría remota retrospectiva pues al parecer de los reguladores europeos ésta es menos lesiva que aquella por habilitar la identificación de personas de manera diferida en el tiempo.

Sin apropiar una visión crítica, las regulaciones de América Latina ven la regulación europea una suerte de estándar de oro, pese a tratarse de un marco normativo ampliamente criticado por organizaciones de la sociedad civil que defienden derechos humanos[17] que, en este punto en concreto, pidieron la **prohibición total de los sistemas de biometría remota**, en vivo y retrospectiva, por ser incompatibles con los derechos humanos y habilitar a los Estados al despliegue de verdaderos sistemas de vigilancia masiva de la población.

---

[15] Câmara de Deputados, projeto de lei 2338/2023 "Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana". En: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2868197&filename=PL%202338/2023

[16] Gianini, A.; Tas, S. (Verfassungsblog, December 10, 2024). AI Act and the prohibition of Real-Time Biometric Identification. En: https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/

[17] Bits of Freedom (November 25, 2022). A limited ban on biometric surveillance undermines its own potential. En: https://www.bitsoffreedom.nl/2022/11/25/a-limited-ban-on-biometric-surveillance-undermines-its-own-potential/ ; Joint Civil Society recommendations for an EU Articiail Intelligence Act for Fundamental Rights, "Prohibit all remote biometric identificacion (RBI) In publicly accessible spaces". En: https://edri.org/wp-content/uploads/2022/05/Prohibit-RBI-in-publicly-accessible-spaces-Civil-Society-Amendments-AI-Act-FINAL.pdf

Para dichas organizaciones, no tiene sentido diferenciar el tratamiento a nivel regulatorio entre un tipo de biometría y otro, pues ambas tienen un impacto indiferenciado en tanto amenazan con derechos críticos para un espacio cívico saludable, como la expectativa de privacidad, el anonimato, entre otros. Sin importar las críticas sobre el tratamiento de este tipo de IA de alto riesgo que puede ser trasladada a las tareas de lucha contra el terrorismo, los Estados de la región han replicado un enfoque incompatible con la protección de derechos.

Advertimos distintos riesgos asociados a estos enfoques regulatorios pues:

- El despliegue de **sistemas de biometría remota**, en tanto que modalidad de la **IA predictiva**, deberían ser objeto de moratorias cuando se busca su adopción para tareas en la lucha contra el terrorismo.
- Las iniciativas regulatorias de la región dan **luz verde al uso de sistemas de IA de alto riesgo**, que lo son precisamente por representar una amenaza al ejercicio de los derechos humanos, amplificando el riesgo intrínseco que suponen las tareas de lucha contra el terrorismo que, según esta misma Relatoría, suelen ser abusadas por los Estados para asentar y legitimar regímenes de vigilancia masiva de la población.
- Se autoriza al uso de una modalidad riesgosa de la IA –insertada en tecnologías de identificación biométrica a distancia- **sin que se robustezcan las garantías de protección a derechos** más a allá de menciones genéricas al debido proceso y la no discriminación.
- La ausencia de garantías concretas y operativas en el marco del uso de la IA que automatiza el funcionamiento de los sistemas de biometría a distancia y en tiempo real o retrospectiva –peligrosa por el impacto agravado de las predicciones que realiza respecto a potenciales sospechosos– **socava la vigencia de los derechos humanos** y no debería estar autorizado su uso estatal para la lucha contra el terrorismo sin garantías debidas ni salvaguardas.

Los **sistemas de biometría –en tiempo real o retrospectiva– para la lucha contra el terrorismo** son problemáticos pues legitiman la masificación de sistemas de vigilancia multimodal, entre los que se incluyen las tecnologías de reconocimiento facial, y de otras formas de biometría corporal, que debilitan las garantías de cientos de personas presentes en el espacio público y privado donde cámaras con todo tipo de cobertura y capacidad de grabación y retención de cientos de horas de imágenes amplifican el apetito por los datos y su explotación intensiva por los Estados.

Sobre este fenómeno la Relatoría Especial contra el Terrorismo ya advirtió en su informe cómo las tecnologías de identificación biométrica han trascendido a tareas asociadas a la seguridad ciudadana, como la identificación civil, la justicia criminal y el manejo de fronteras. Y enmarcadas en ese fenómeno de naturalización de una tecnología invasiva y riesgosa desde la perspectiva de derechos, se ha extendido la biometría también a la lucha contra el terrorismo en ocasiones, con objetivos legítimos, pero en otros, para justificar violaciones masivas a los derechos humanos.[18]

[18] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism Fionnuala Ní Aoláin, "Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent

Más aún, en su reporte A/HRC/53/39 esta misma Relatoría advirtió por el uso de sistemas de biometría en la lucha contra el terrorismo incluso con impulso de las Naciones Unidas, **sin que en dicho terreno se haya profundizado lo suficiente en estándares regulatorios y legales** necesarios para alinear su despliegue a obligaciones internacionales en derechos humanos.[19]

La potencial propagación de esta tecnología para tareas complejas y sensibles para la lucha contra el terrorismo se encuentra paralelamente aunada a la presión de países como los Estados Unidos sobre países de América Latina para pactar el **intercambio de datos biométricos en beneficio del país del Norte Global**, para facilitar supuestamente la lucha contra delitos domésticos y la identificación de criminales bajo la narrativa de la lucha contra las drogas. Esta presión genera un incentivo enfocado en la mayor captura de datos biométricos, dando sentido y urgencia a las disposiciones regulatorias que legitiman su masificación –como las que vimos anteriormente–.

Los Estados Unidos han impuesto a varios países, como condición para la negociación de aranceles, la entrega de datos biométricos[20]. Por ahora, países como **Colombia[21], Chile[22], Ecuador[23] y Argentina[24]** han accedido al intercambio de datos biométricos de la población bajo acuerdos que, en buena medida, son secretos en su contenido, alcance y propósito.[25] Países como **México** se encuentran analizando si acceder o no a la entrega de datos biométricos[26] al tiempo que recientemente oficializó, en el marco de un paquete

---

extremism", A/HRC/52/39, March 2023, paragraph 9; 18 and following. En: https://docs.un.org/en/A/HRC/52/39

[19] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism Fionnuala Ní Aoláin, "Human rights implications of the development, use and transfer of new technologies in the context of counter-terrorism and countering and preventing violent extremism", A/HRC/52/39, March 2023. See paragraph 23 En: https://docs.un.org/en/A/HRC/52/39

[20] Torres, N. (CW+, Junio 30, 2025). Los peligrosos escenarios del acuerdo biométrico entre EEUU y Colombia. En: https://cwmas.com.co/unidad-investigativa/2025/06/30/los-peligrosos-escenarios-del-acuerdo-biometrico-entre-ee-uu-y-colombia/

[21] Embajada de Colombia en Estados Unidos (Marzo 27, 2025). Migración, seguridad, comercio y lucha contra las drogas: temas del encuentro de la Canciller Laura Sarabia y la Secretaria de Seguridad Nacional de los Estados Unidos, Kristi Noem). En: https://estadosunidos.embajada.gov.co/newsroom/news/migracion-seguridad-comercio-y-lucha-contra-las-drogas-temas-del-encuentro-de-la

[22] La Nación (Agosto 3, 2025). La alianza de ICE con un país latino para avanzar un nuevo acuerdo sobre seguridad migratoria en EEUU. En: https://www.lanacion.com.ar/estados-unidos/migraciones/avanza-el-ice-ahora-se-unio-con-un-pais-latino-para-firmar-un-nuevo-acuerdo-sobre-seguridad-nid31072025/

[23] Primicias (Agosto 14, 2025). Estados Unidos y Ecuador compartirán información biométrica para identificar criminales, ¿qué son estos datos y qué comprende el acuerdo firmado?. En: https://www.primicias.ec/seguridad/cooperacion-informacion-biometrica-estados-unidos-ecuador-acuerdos-chile-colombia-101969/

[24] Dolabjian, C. (La Nación, Julio 28, 2025). Kristi Noem, sobre el acuerdo que firmó para eliminar las visas: "Es muy difícil que sea en menos de un año". En: https://www.lanacion.com.ar/politica/kristi-noem-sobre-el-acuerdo-que-firmo-para-eliminar-las-visas-es-muy-dificil-que-sea-en-menos-de-un-nid28072025/

[25] Torres, N. (CW+, Junio 30, 2025). Los peligrosos escenarios del acuerdo biométrico entre EEUU y Colombia. En: https://cwmas.com.co/unidad-investigativa/2025/06/30/los-peligrosos-escenarios-del-acuerdo-biometrico-entre-ee-uu-y-colombia/

[26] Calderón, V. (CNN, Abril 1, 2025). Sheinbaum niega haber firmado acuerdo para compartir datos biométricos con EEUU, pero no descarta tratar el tema. En: https://cnnespanol.cnn.com/2025/04/01/mexico/sheinbaum-niega-firma-acuerdo-datos-biometricos-ee-uu-orix

legislativo de seguridad[27], y con objeciones de organizaciones en derechos humanos, la masificación obligatoria de un sistema de identificación biométrica estatal que capturará datos faciales, dactilares, entre otros.

Manifestamos nuestra preocupación y llamamos la atención de esta Relatoría para prestar atención al **contexto geopolítico actual** en las relaciones diplomáticas de países de América Latina y Estados Unidos, y que supone una presión sobre la independencia regulatoria de países soberanos donde los acuerdos de negociación comercial se condicionan a la entrega del conjunto de datos más sensibles que tienen en sus manos los Estados, como lo son los datos biométricos, y de presión al despliegue de tecnologías que intervienen en el ciclo de vida de su tratamiento, captura, procesamiento y almacenamiento.

B. El uso dual de la IA de alto riesgo y sistemas de reconocimiento facial: de la seguridad ciudadana, a la lucha contra el terrorismo

Pese a ello, en América Latina el uso de sistemas de biometría a distancia o remota ya está siendo desplegada a través de **tecnologías de reconocimiento facial** que cada vez más se masifican en el marco de las tareas para la seguridad ciudadana, con los riesgos que esto implica. Por lo que su extensión a las tareas de lucha contra el terrorismo parece, en la práctica, un **potencial uso dual** de una tecnología que ya ha sido apropiada y empleada por las autoridades públicas de varios países de la región.

En la región, el caso de **Brasil** es preocupante por la masividad del uso de sistemas de reconocimiento facial para tareas de seguridad ciudadana. Organizaciones locales como O Panóptico, que se dedican a monitorear su despliegue a nivel nacional y local, han advertido[28] que se han instalado desde 2019 y hasta 2025 aproximadamente 337 sistemas de reconocimiento facial en el país para tareas de seguridad ciudadana. Dicho uso se ha caracterizado por (i) la falta de transparencia de las autoridades sobre su despliegue, (ii) el incumplimiento sistemático de la ley general de protección de datos, (iii) la justificación amparada en la prevención del crimen, la identificación de prófugos e identificación de personas desaparecidas, sin que medien garantías apropiadas frente a errores o predicciones sesgadas de la IA, y (iv) su adquisición poco transparente.

De hecho, en el país, los sistemas de reconocimiento facial proliferan en todo tipo de espacios públicos, no solo las tradicionales plazas públicas, sino también en escenarios deportivos, sistemas de transporte público, y escenarios para los espectáculos artísticos bajo la narrativa de la securitización[29] enfocados en la lucha contra el crimen. Los **errores de dichos sistemas**, masificados en ciudades como Sao Paulo, han conducido a las autoridades a la

---

[27] Vila, E. (El País, Junio 28, 2025). Del espionaje a la CURP biométrica: las claves para entender las leyes de seguridad que se discuten en el Congreso. En: https://elpais.com/mexico/2025-06-28/del-espionaje-a-la-curp-biometrica-las-claves-para-entender-las-leyes-de-seguridad-que-se-discuten-en-el-congreso.html

[28] NUNES, Pablo et al. Mapeando a vigilância biométrica [livro eletrônico]: levantamento nacional sobre o uso do reconhecimento facial na segurança pública. Rio de Janeiro: CESeC, 2025. En: https://drive.google.com/file/d/1bN2ssBp_dMiih8YOUonLhGl_5jRoNe5s/view

[29] Nunes, P.; Casteliano, C. (The Conversation, May 26th, 2025). Erros, abusos, injusticias: maioria dos sistemas de reconhecimento facial no Brasil atua sem transparencia. En: https://theconversation.com/erros-abusos-injusticas-maioria-dos-sistemas-de-reconhecimento-facial-no-brasil-atua-sem-transparencia-256417

detención de una mujer en estado de embarazo, acusada injusta e infundadamente de ser criminal[30] –situación que la condujo a un parto prematuro-, y a la detención por más de diez horas de una persona de la tercera edad acusada injustamente del crimen de violación y fuga.[31]

En países como **Argentina**, se ha usado sistemas de reconocimiento facial para identificar a personas con orden judicial de captura en la Ciudad de Buenos Aires, poniendo en evidencia muchos de los problemas asociados a su despliegue y los impactos en derechos humanos que serían amplificados en su **potencial uso dual** para la lucha contra el terrorismo.

En 2019 el gobierno de la Ciudad de Buenos Aires comenzó a utilizar un software de reconocimiento facial en tiempo real, aplicado a algunas cámaras del sistema de vigilancia, con el objetivo de identificar a personas con orden de captura por parte de la justicia. Esta herramienta tecnológica fue adquirida e implementada **sin que se produjeran estudios de impacto ni se estableciera un sistema de supervisión**. Tampoco se brindó información sobre el software y sus características.

Luego de algunos casos de detenciones de personas erróneamente identificadas por el sistema como prófugas, la organización ODIA (Observatorio del Derecho Informático en Argentina) presentó una medida cautelar a la que se sumó luego el CELS. Se pedía la suspensión del sistema dados los antecedentes registrados en otros países de mal funcionamiento, sesgos raciales, etc. La Justicia accedió a suspender el sistema temporalmente e inició una investigación sobre su implementación. Allí se descubrió no sólo que las bases de datos estaban desactualizadas, generando altos riesgos de detenciones erróneas, sino que además se identificó que el acuerdo que el gobierno de la Ciudad había firmado con el Registro Nacional de las Personas (RENAPER) para acceder a la base nacional de datos biométricos con el fin de identificar prófugos estaba siendo **utilizado para muchas otras cosas que hasta el momento no han sido aclaradas**. La base de prófugos consta de 40 mil personas, y se registraron consultas por más de siete millones de personas.

Frente a esta situación el poder judicial confirmó la suspensión del sistema, y ordenó una serie de medidas que deben tomarse para que vuelva a ponerse en funcionamiento. Una de ellas es la evaluación de impacto del software adquirido. Sin embargo, transcurridos casi seis años y a pesar del requerimiento judicial, **ni el gobierno ni la empresa licenciataria han informado de qué software se trata**. Es decir, no han brindado ni siquiera la información más básica para poder realizar un estudio de su impacto, ni de evaluación de efectividad del sistema. **La empresa proveedora del sistema de reconocimiento facial** se niega a entregar datos sobre el funcionamiento del software que permitirían discernir los potenciales riesgos de su uso. Por esta negativa a brindar información tanto del Estado como de la empresa, la causa judicial se encuentra paralizada desde hace dos años.

---

[30] Audi, A. (Abril 16, 2025). Smart Sampa: Grávida é presa em posto de saúde e acaba tendo parto prematuro. En: https://apublica.org/2025/04/smart-sampa-gravida-e-presa-em-posto-de-saude-e-acaba-tendo-parto-prematuro/

[31] Araújo, M.; Vespa, T. (UOL, Abril 13, 2025). Reconhecimento facial de SP confunde idoso com estuprador foragido. En: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2025/04/13/reconhecimento-facial-de-sp-confunde-idoso-com-estuprador-foragido.htm

C. *Nueva oleada de regulación en materia de inteligencia o de lucha contra el terrorismo*

En **Argentina**, en julio de 2024, el Ministerio de Seguridad de la Nación, a través de la resolución 710/2024, creó la Unidad de Inteligencia Artificial Aplicada a la Seguridad (UIAAS). La norma es extremadamente vaga, pero se anuncia que la unidad tendrá atribuciones para predicción de delitos, perfilado de personas, análisis de casos y detección de fraudes. Entre sus atribuciones se encuentra la de realizar las tareas de **ciberpatrullaje**[32], confirmando que la IA se aplicará a este tipo de tareas de vigilancia.

En la Argentina se ha naturalizado el término ciberpatrullaje, una atribución relativamente nueva de las fuerzas de seguridad cuya regulación avanza sobre los hechos consumados: las policías hacen ciberpatrullaje de hecho, y luego aparecen algunos protocolos o normas que las habilitan a hacerlo, sin que se establezcan controles y no garantías para los ciudadanos.

En su uso más generalizado, el **ciberpatrullaje** se asienta sobre una concepción equívoca sostenida por los gobiernos de la región: que la policía puede realizar tareas "preventivas" en el espacio público digital, de la misma forma en que lo hace en el espacio público físico con su sola presencia[33]. Esto autoriza a los integrantes de las fuerzas de seguridad a realizar monitoreos de fuentes abiertas (plataformas, redes sociales, páginas de internet) sin necesidad de que exista una hipótesis delictiva previa. Desde el punto de vista de los derechos humanos, esto **no es prevención del delito, sino vigilancia masiva**, y debe ser regulada para proteger la privacidad y la libertad de expresión en entornos digitales[34].

En relación con la cuestión del terrorismo, el foco del debate no sería el mismo, ya que el monitoreo de fuentes abiertas con orden judicial o ante una sospecha fundada de actividades terroristas sería una tarea de investigación válida. Sin embargo, hay indicios de una **creciente automatización** de estas tareas, es decir, del uso de tecnologías de inteligencia artificial para realizar el escaneo de las fuentes abiertas, con lo que se reproducen en este ámbito la opacidad y los riesgos ya mencionados.

Desde el momento en que se dio a conocer la resolución 710/2024, varias organizaciones de la sociedad civil expresamos nuestras preocupaciones sobre este paquete de vigilancia. En agosto de 2024 un consorcio de organizaciones realizamos un pedido de información para que el Ministerio de Seguridad explique varios puntos confusos, como el marco normativo aplicable a estas actividades o los modos de supervisión, y que especifique el significado asignado a una serie de palabras o expresiones ambiguas e indefinidas.

---

[32] Cuzcano, X. (Derechos Digitales, Mayo 9, 2025. Ciberpatrullaje: cuando vigilar se justifica en nombre de la seguridad. En: https://www.derechosdigitales.org/recursos/ciberpatrullaje-cuando-vigilar-se-justifica-en-nombre-de-la-seguridad/

[33] Camacho, L. (CELE, 2024). Ciberpatrullaje en Argentina: Análisis de una Resolución problemática. En: https://observatoriolegislativocele.com/ciberpatrullaje-en-argentina-analisis-de-una-resolucion-problematica-por-lucia-camacho-g/

[34] Cousiño, M (El Grito del Sur, Julio 2, 2025) Ciberpatrullaje sin límites: nuevas formas de vigilancia y el intento de acallar voces. En: https://elgritodelsur.com.ar/2025/07/ciberpatrullaje-sin-limites-formas-vigilancia-intento-acallar-voces/

La respuesta del Ministerio de Seguridad fue que se encuentran "trabajando en la construcción de herramientas y normativas complementarias que den cuenta de lo aquí dicho. Se asegura el apego irrestricto a las normas constitucionales vigentes". Es decir, la norma entró en vigencia sin que se especifiquen correctamente sus alcances e implicancias. No se sabe, por ejemplo, a qué se refiere concretamente **el Estado cuando habla de Inteligencia Artificial** en el marco de esta resolución. Un segundo pedido de información realizado por la organización ODIA en mayo de 2025 recibió una respuesta similar. También los pedidos realizados desde el periodismo recibieron como respuesta que "se está trabajando" en el tema, o directamente no fueron respondidos.

En **Ecuador**, por otro lado, se aprobó recientemente y de manera expedita una nueva Ley Orgánica de Inteligencia[35] en el marco de la lucha contra el crimen organizado calificado por el presidente como "organizaciones terroristas"[36] cuya actuación criminal, de hecho, motivó a la declaratoria de un conflicto armado interno en 2024, la cual habilita el despliegue del Ejército Nacional en las ciudades del país y le delega facultades para la detención de personas, entre otros.

Dicha declaratoria se encuentra todavía vigente pues fue ratificada el pasado 16 de junio de 2025[37]. La Corte Constitucional de ese país consideró que la declaratoria de un conflicto armado interno era innecesaria y ha sido instrumentalizada para habilitar la declaratoria de estados de excepción que traen consigo la restricción de derechos fundamentales en el país.[38]

En ese contexto social y político, la nueva Ley Orgánica de Inteligencia no solo **elimina garantías básicas de revisión judicial** de órdenes de interceptación de las comunicaciones, ordena la entrega de cualquier base de datos en manos de personas jurídicas y naturales de cualquier sector –sin que puedan oponerse– cuando sea de interés del ente rector del sistema de inteligencia, sino que además habilita a la adquisición y uso incondicional de cualquier tipo de **software y hardware** para habilitar a la interceptación de las comunicaciones de las personas, lo que **incluiría la compra de tecnologías de IA** para dichos fines con la garantía de la opacidad en el uso de recursos asignados a dicho fin, pues la ley protege tal adquisición a través de la figura de los "gastos reservados".

---

[35] Registro oficial, órgano de la República de Ecuador, "Ley Orgánica de Inteligencia", En: https://strapi.lexis.com.ec/uploads/Registro_Oficial_Ano_1_Cuarto_Suplemento_No_57_10_de_junio_de_2025_6565dee8a1.pdf

[36] BBC News Mundo (Enero 10, 2024). Qué poder tienen las bandas que Ecuador califica como "organizaciones terroristas". En: https://www.bbc.com/mundo/articles/c1vy2ylnz5go

[37] Rubio, E. (GK, Agosto 4, 2025). 554 días de conflicto armado interno: resultados a medias y cuestionamientos. En: https://gk.city/2025/08/04/como-ha-sido-conflicto-armado-interno-ratificacion-ley-solidaridad-nacional-daniel-noboa/

[38] Infobae (Junio 11, 2025). La Corte Constitucional de Ecuador anuló la aplicación del Estado de excepción en las cárceles del país. En: https://www.infobae.com/america/america-latina/2025/06/11/la-corte-constitucional-de-ecuador-anulo-la-aplicacion-del-estado-de-excepcion-en-las-carceles-del-pais/; DW (Mayo 11, 2024). Corte Ecuador declara inconstitucional estado de excepción. En: https://www.dw.com/es/corte-de-ecuador-declara-inconstitucional-%C3%BAltimo-estado-de-excepci%C3%B3n-decretado-por-noboa/a-69051827

El Reglamento[39] de la Ley Orgánica, además, ratifica la ausencia de controles judiciales sobre órdenes de interceptación y consolida la opacidad sobre las actividades de inteligencia –de las que el ente rector rendirá esporádicamente cuentas ante la Asamblea Nacional, exceptuando asuntos asociados al uso de "gastos reservados"-.

Un análisis de Derechos Digitales[40] sobre el contenido del proyecto que luego se convirtió en Ley concluye que se trata de un cuerpo normativo **contrario a estándares internacionales,** como los *Principios de Twshane* sobre acceso a la información aplicable a las tareas de inteligencia, así como resulta **inconvencional** de cara al reciente fallo de la Corte Interamericana de Derecho Humanos**, CAJAR vs Colombia**[41], que prevé, entre otros, el acceso a la información y la transparencia como un mecanismo crítico para el escrutinio de las facultades de inteligencia en manos de las autoridades, en especial cuando éstas son ejercidas a través del uso de tecnologías digitales.[42]

Recientemente, la Corte Constitucional del país emitió auto de admisibilidad de las demandas que acusan la inconstitucionalidad de la Ley Orgánica y el Reglamento, y suspendió como medida cautelar varios de los artículos que conceden poderes extraordinarios al ejecutivo para interceptar las comunicaciones, incluyendo el artículo 43 que habilita a la compra indiscriminada de software y hardware para "recopilar, analizar y utilizar información para generar inteligencia y contrainteligencia".[43]

En **Chile,** la Ley de Antiterrorismo se reformó a fines de 2024[44]. El contenido de dicho cuerpo normativo se actualizó, según el gobierno nacional, para "mejorar las condiciones de lucha contra el crimen organizado".[45] La ley amplía la definición de delito terrorista, crea el delito de asociación terrorista, sanciona casos de terrorismo individual, crea el delito de

[39] Reglamento General a la Ley Orgánica de Inteligencia, En: https://strapi.lexis.com.ec/uploads/Decreto_Ejecutivo_52_20250614181115_20250614181121_20250614181156_ad448932bb.pdf
[40] Camacho L. (Derechos Digitales, 2025). En Ecuador se discute una ley de inteligencia incompatible con los derechos humanos. En: https://www.derechosdigitales.org/wp-content/uploads/Analisis-Proyecto-de-Ley-Inteligencia-Ecuador-2025.pdf
[41] Camacho, L. (Derechos Digitales, Julio 12, 2024). Histórica sentencia de la Corte Interamericana de Derechos Humanos: la protección de datos aplica a las tareas de inteligencia. 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/
[42] Corte Interamericana de Derechos Humanos, Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia. En: https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf
[43] Corte Constitucional Ecuador, Admisión de demandas y suspensión provisional de normas en Leyes de reciente promulgación. En: https://www.corteconstitucional.gob.ec/admision-de-demandas-y-suspension-provisional-de-normas-en-leyes-de-reciente-promulgacion/
[44] Ley 21.732 que "determina conductas terroristas, fija su penalidad y deroga la Ley N° 18.314. En: https://www.bcn.cl/leychile/navegar?idNorma=1211036
[45] Ministerio del Interior de Chile (Febrero 4, 2025). Presidente Boric promulga nueva Ley Antiterrorista: "El terrorismo no sólo es un ataque contra personas inocentes, es una agresión a la libertad, a la democracia y a la convivencia pacífica". En: https://www.interior.gob.cl/noticias/2025/02/04/presidente-boric-promulga-la-nueva-ley-antiterrorista-el-terrorismo-no-solo-es-un-ataque-contra-personas-inocentes-es-una-agresion-a-la-libertad-a-la-democracia-y-a-la-convivencia-pacifica/

favorecimiento de asociación terrorista, y amplía el conjunto de **herramientas especiales de investigación**.[46]

En Chile, las leyes de antiterrorismo han sido usadas en el pasado para criminalizar y perseguir a grupos y líderes Mapuche. En 2014[47] la Relatoría de ONU para la Promoción y Protección de los Derechos Humanos y las Libertades Fundamentales en la lucha contra el Terrorismo advirtió sobre el **abuso en el uso de la Ley Antiterrorismo** de entonces para judicializar y reprimir las protestas Mapuche; y en 2016[48], diversos expertos de la ONU volvieron a advertir sobre el abuso e **instrumentalización de dicha legislación** para perseguir el ejercicio legítimo de la protesta pacífica y mayoritaria de los Mapuche, y sobre los riesgos asociados a estos marcos regulatorios que debilitan "la posibilidad de un juicio justo" al legitimar la restricción injusta de derechos en ausencia de garantías básicas, como la presunción de inocencia o el debido proceso.[49]

De hecho, en 2021[50] y 2022[51] se mantuvieron las tensiones entre el gobierno nacional y grupos Mapuche presentes en la zona de la Araucanía, donde la narrativa oficial sigue acusando a grupos y liderazgos del pueblo indígena de ser un grupo terrorista. Ante el escalamiento sostenido de la situación con los pueblos Mapuche, se aprueba la nueva Ley Antiterrorista que, aunque la narrativa oficial no lo advierta así, buscará ser empleada en ese contexto específico.

Así las cosas, el conjunto de nuevas herramientas especiales de investigación que trajo consigo la nueva ley, habilita a la intervención de las comunicaciones "mediante tecnologías que simulen sistemas de transmisión de las telecomunicaciones u otras tecnologías similares" (art. 19). Entre las tecnologías explicitadas por la ley se habilita al uso de IMSI-Catchers, riesgosos en tanto habilitan a la **vigilancia masiva de personas** sin relación a una investigación judicial en curso[52]. Pero el contenido de la ley habilitaría, por su redacción vaga, a la adquisición de cualquier tecnología con dicha capacidad, **entre las que se incluiría a la IA**.

---

[46] Gob.CL (Febrero 4, 2025). Ley Antiterrorista: Promulgamos nueva legislación moderna, eficaz y democrática contra el terrorismo. En: https://www.gob.cl/noticias/promulgacion-nueva-ley-antiterrorista-legislacion-moderna-eficaz-legitima/
[47] Cayuqueo, P. (Agosto 1, 2013). La fábula del terrorismo Mapuche. En: https://www.latercera.com/voces/la-fabula-del-terrorismo-mapuche/
[48] Comunicado de Prensa (Octubre 6, 2017). Expertos de la ONU urgen a Chile no usar Ley Antiterrorista contra indígenas Mapuche. En: https://www.ohchr.org/es/press-releases/2017/10/un-experts-urge-chile-not-use-anti-terrorism-law-against-mapuche-indigenous
[49] Comunicado de Prensa (Octubre 6, 2017). Expertos de la ONU urgen a Chile no usar Ley Antiterrorista contra indígenas Mapuche. En: https://news.un.org/es/story/2017/10/1387431
[50] Newman, L .(Aljazeera, April 12, 2021). A journey through Chile's conflict with Mapuche rebel groups. En: https://www-aljazeera-com.translate.goog/features/2021/4/12/a-journey-through-chiles-conflict-with-mapuche-resistance-groups?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc
[51] Carmona, C. (Noviembre 22, 2022). Los riesgos de hablar de "terrorismo" en la Araucanía. En: https://www.ciperchile.cl/2022/11/22/los-riesgos-de-hablar-de-terrorismo-en-la-araucania/
[52] Flóres, M. (Derechos Digitales, Enero 17, 2025). Vigilancia estatal: Los riesgos de los IMSI Catchers. En: https://www.derechosdigitales.org/24747/vigilancia-estatal-los-riesgos-de-los-imsi-catchers-en-chile/

3. Recomendaciones

En consideración de la información anterior, recomendamos a la Relatoría Especial para la lucha contra el terrorismo en la elaboración de su informe:

A. Aproximar la discusión sobre nuevos paradigmas en la lucha contra el terrorismo, y cómo la IA, o cualquier tecnología digital con una arquitectura y capacidades enfocadas en la recoleccion o explotación masiva de información, **pueden maximizar las facultades preexistentes de vigilancia masiva** en manos de las autoridades, bajo escenarios habilitadores de la opacidad y secreto generalizados sobre este tipo de prácticas.
B. Aproximar su análisis sobre el estado de la cuestión en América Latina considerando incluso cómo las **tendencias en la región viran a la erosión de las garantías legales preexistentes** en marcos legislativos de seguridad, la inteligencia y lucha contra el terrorismo, y se legitima la expansión de tecnologías problemáticas, como la biometría remota en tiempo real y retrospectiva para su potencial uso dual también en la lucha contra el terrorismo y otros fenómenos emergentes, como el ciberpatrullaje.
C. Cuestionar por su impacto en derechos humanos la aproximación regional a la **regulación de la IA que imita el modelo de regulación en Europa** que habilitó al uso de alto riesgo de sistemas de IA para la operación de sistemas de biometría remota en tiempo real y retrospectiva.
D. Prestar atención a la **deficiencia continua de garantías necesarias en derechos humanos** todavía ausentes en los marcos de regulación de las tareas de inteligencia, y lucha contra el terrorismo, como el debido proceso, igualdad y no discriminación, protección de datos, privacidad, entre otros.
E. Prestar atención a la **heterogeneidad normativa** que persiste en la región sobre asuntos regulatorios críticos para el despliegue y masificación de tecnologías como la IA y otras, como la biometría, en la lucha contra el terrorismo, como las legislaciones sobre protección de datos y su aplicación respecto a los Estados cuando actúan en calidad de responsables del tratamiento de datos de la población.
F. Llamar la atención a la importancia de imponer **moratorias en el despliegue de sistemas de IA para la lucha contra el terrorismo**, y a que dicha moratoria no sea levantada hasta que obligaciones en materia de derechos humanos sean satisfactoriamente reguladas respecto de actores estatales y empresas.
G. Urgimos a la Relatoría Especial a encabezar discusiones enfocadas en la **prohibición de sistemas de IA de alto riesgo de naturaleza predictiva –como la biometría remota en tiempo real o retrospectiva–**, que por su diseño y arquitectura propensa a los errores probabilísticos deben ser excluidos de despliegue en la lucha contra el terrorismo.

4. Sobre nosotros

El ***Centro de Estudios Legales y Sociales***[53] –CELS– es una organización de derechos humanos argentina creada en 1979, durante la última dictadura militar, que promueve la protección de los derechos y su ejercicio efectivo, la justicia y la inclusión social, a nivel nacional e internacional.

Derechos Digitales[54] es una organización de alcance latinoamericano, independiente y sin fines de lucro, fundada en 2005 y que tiene como objetivo fundamental el desarrollo, la defensa y la promoción de los derechos humanos en el entorno digital.

Fundación Vía Libre[55] es una organización civil sin fines de lucro nacida en la ciudad de Córdoba, Argentina, en el año 2000. Inicialmente enfocada en políticas públicas de Software Libre para la difusión del conocimiento y el desarrollo sustentable, la Fundación orientó su misión a temáticas más amplias de derechos sociales, económicos y culturales y derechos civiles y políticos en entornos mediados por tecnologías digitales.

[53] https://www.cels.org.ar/web/
[54] https://www.derechosdigitales.org/
[55] https://www.vialibre.org.ar/