

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

Concepto técnico de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos en Colombia respecto a la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

Previo a abordar el contenido del proyecto de reforma de ley estatutaria en relación con los estándares internacionales de derechos humanos es pertinente mencionar los pronunciamientos nacionales e internacionales sobre la Ley Estatutaria 1621 de 2013. Esto reflejará la idoneidad de la reforma y el avance histórico que supondría su aprobación.

Según el informe de la Comisión para el Esclarecimiento de la Verdad, la Convivencia y la No Repetición (CEV) creada en el marco de la firma del Acuerdo Final de Paz de 2016, la inteligencia, principalmente la militar, jugó un papel significativo en la identificación y neutralización de lo que el Estado consideraba amenazas bajo una concepción del “enemigo interno”. Dicho enfoque, se extendió a actividades que involucraban la estigmatización y criminalización de movimientos políticos y sociales, así como de personas defensoras de derechos humanos, bajo la presunción de vínculos con grupos armados y terroristas.[1] Hasta 2013, dichas actuaciones se regulaban por el Ministerio de Defensa Nacional, el Departamento Administrativo de Seguridad (DAS) y excepcionalmente, por la jurisprudencia de la Corte Constitucional, sin un marco legal unificado.

En 2013, se aprobó la Ley Estatutaria 1621 para regular a los organismos de inteligencia y contrainteligencia que representó la primera legislación y un avance en la materia. A pesar de las reformas introducidas, según la CEV, se siguieron reportando abusos en el uso de la inteligencia militar, incluyendo seguimientos, interceptaciones y perfilamiento de personas consideradas opositores del gobierno, así como periodistas, lo cual muestra deficiencias en la implementación y supervisión de las normativas establecidas por la ley.[2] Derivado de ello, la CEV, en su informe final recomendó cambiar la perspectiva de la inteligencia, para no estigmatizar a la población civil;[3] garantizar el direccionamiento civil sobre las Fuerzas Militares, la Policía y los organismos civiles de inteligencia;[4] fortalecer los controles preventivo, penal, disciplinario y fiscal y la supervisión democrática de las Fuerzas Militares, la Policía y los organismos de inteligencia para mitigar factores de riesgo y hacer frente a la impunidad y;[5] derogar la disposición en la Ley de Inteligencia y Contrainteligencia que establece un plazo de confidencialidad de 30 años y mantener un plazo máximo de 15 años.[6]

Estas alegaciones sobre el uso arbitrario de la inteligencia también han sido recibidas por órganos internacionales, que han recomendado incorporar estándares de derechos humanos en la gestión de inteligencia. El Comité de Derechos Humanos mostró preocupación por las

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

alegaciones que existen por actividades ilegales de vigilancia contra defensores y reporteros.[7] La Relatora sobre el derecho a la privacidad mostró inquietud por la vigilancia contra la periodista Claudia Julieta Duque Orrego debido a su labor en defensa de los derechos humanos, señalando que las medidas de protección podrían estar siendo utilizadas para monitorearla, afectando su privacidad y trabajo.[8] En consonancia, ONU Derechos Humanos en su informe sobre la situación de derechos humanos en Colombia de 2023, recomendó que las entidades de inteligencia integren efectivamente los estándares internacionales de derechos humanos en su doctrina e instrumentos misionales, reflejándolos en los ordenamientos normativos y las operaciones de inteligencia.[9]

En 2020, la sociedad civil y organizaciones de derechos humanos pusieron en conocimiento de la Comisión Interamericana de Derechos Humanos (CIDH) el uso de *softwares* y tecnología de vigilancia sin un adecuado control de acuerdo con los derechos humanos.[10] Ese mismo año, la CIDH mencionó en el informe sobre su visita a Colombia[11], su preocupación por las reiteradas denuncias sobre el perfilamiento de personas usuarias de redes sociales, participantes o no de las protestas a quienes se les caracterizaba de manera “genérica a través de términos como “terrorismo”, “vandalismo” o “criminales””.

Asimismo, en el caso *CAJAR vs. Colombia*, la Corte Interamericana realizó un análisis de la Ley 1621, condenando a Colombia por no cumplir con los estándares de derechos humanos. La Corte destacó que la ambigüedad de la ley permite un uso indiscriminado de las funciones de inteligencia y subrayó la necesidad de establecer registros de las actividades de inteligencia, así como de implementar un control judicial. Además, concluyó que el control legislativo existente es ineficaz y que las personas afectadas no tienen acceso a su información personal. [12] Por lo tanto, la Corte ordenó diversas medidas para garantizar la no repetición del uso arbitrario de la inteligencia, incluida la reforma de la Ley 1621 y su decreto reglamentario 2147 de 2013. [13] Es necesario destacar que las sentencias de la Corte IDH son de cumplimiento obligatorio de conformidad con el artículo 68.1[14] de la Convención Americana sobre Derechos Humanos ratificada por Colombia el 28 de mayo 1973, así como por ser parte del bloque de constitucionalidad en la Constitución de Política de Colombia con base a su artículo 93. [15]

Por último, el 4 de septiembre de 2024, el presidente Gustavo Petro dio a conocer que la Dirección de Inteligencia Policial (DIPOL), adquirió un malware para espiar en medio del estallido social en 2021 por un valor de Por estos hechos, ONU Derechos Humanos en Colombia refirió que este spyware vulnera gravemente la privacidad, libertad de expresión y otros derechos humanos. Asimismo, instó a las autoridades a avanzar con diligencia en la investigación para esclarecer los hechos, así como recordó que el proyecto de reforma a la ley de inteligencia incluye garantías que podrían prevenir la adquisición de estas

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

tecnologías en el futuro.[\[19\]](#)

Con estos antecedentes, la propuesta de reforma de la ley contribuye sin duda al cumplimiento de las obligaciones y resoluciones internacionales en la materia, lo que a su vez fortalece el principio de legalidad que rige cualquier sistema de inteligencia, al proporcionar mayor claridad sobre las circunstancias y condiciones en que las autoridades pueden aplicar tales medidas.[\[20\]](#) A continuación, la Oficina destaca aspectos clave que representan un avance en el cumplimiento de estas recomendaciones y resoluciones, tanto nacionales como internacionales, e incluye sugerencias para reforzar estos progresos, asegurando que la reforma de la ley tenga un enfoque integral en la garantía de los derechos humanos.

- 1. Función de la inteligencia y contrainteligencia.** Los artículos 2 al 6 de la propuesta de reforma son esenciales, ya que profundizan en los fines que justifican las funciones de inteligencia y contrainteligencia, estableciendo sus principios rectores, prohibiciones y conceptos clave, como las amenazas que activan estas funciones. A continuación, se destacan diversos aspectos de la propuesta de reforma, junto con las recomendaciones de la Oficina, que aportan mayor claridad y refuerzan un nuevo enfoque: considerar la inteligencia como una herramienta para detectar y prevenir violaciones a los derechos humanos o factores de violencia que generan estas violaciones. Esto marca una diferencia significativa con lo que la CEV identificó como una concepción de las amenazas centrada en la idea de un [\[21\]](#)
- 2. Definición de inteligencia y contrainteligencia y sus fines.** El artículo 2 define la inteligencia y contrainteligencia como funciones públicas orientadas a obtener, procesar, analizar y difundir información útil, preventiva y anticipativa, con el objetivo de identificar oportunidades y amenazas que permitan cumplir con los fines del Estado, tales como el orden constitucional, la seguridad nacional, los regímenes democrático y económico, entre otros, los cuales cómo se detallará tienen como eje central la garantía, respeto y protección de los derechos humanos (ver análisis artículo 3 de la propuesta de reforma en los siguientes párrafos). Además, establece que la contrainteligencia se enfoca en proteger la información recolectada y analizada, así como en prevenir la corrupción, el sabotaje, la infiltración y la cooptación de servidores públicos por organizaciones criminales. Estas definiciones cumplen con los elementos mínimos establecidos en la jurisprudencia del Sistema de Naciones Unidas y la Corte Interamericana.[\[22\]](#) La Oficina destaca que incluir la corrupción como un objetivo de la contrainteligencia es un avance significativo, ya que la normativa vigente no lo contemplaba. Esto está en línea con diversas obligaciones en materia de derechos humanos[\[23\]](#) y refuerza el cambio de enfoque en las funciones de

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

inteligencia y contrainteligencia.

Además, el artículo 2 hace un listado de las amenazas que habilitan la función de inteligencia y contrainteligencia que aporta a fijar límites claros en sus actuaciones. En este sentido, ONU Derechos Humanos recomienda que la definición de terrorismo se ajuste a la Resolución 1566 de 2004 del Consejo de Seguridad, añadiendo el elemento subjetivo de la intencionalidad de causar daño a la vida, la integridad física o la libertad personal, con el propósito de generar un estado de terror en la población o intimidar a un grupo específico. Esta recomendación busca asegurar que la definición de terrorismo esté alineada con el consenso internacional, reduciendo el riesgo de un uso indiscriminado del término.

Ese mismo artículo también incorpora una definición de seguridad humana que va acorde a los estándares más recientes de la Asamblea General de las Naciones Unidas sobre el tema.[\[24\]](#) Aspecto invaluable en el cambio de paradigma pues el artículo 3 de la propuesta de reforma refiere que el enfoque de seguridad humana será el eje central para garantizar el ejercicio pleno de los derechos humanos y la protección de las comunidades y personas.

Por otra parte, el artículo 3 de la propuesta de reforma define los fines legítimos que la inteligencia y contrainteligencia deben proteger mediante la detección y prevención de amenazas internas o externas. Estos fines incluyen el régimen democrático, el orden constitucional y legal, el régimen económico, la seguridad nacional, la defensa nacional, y la seguridad y convivencia ciudadana. Aunque la ley vigente ya contemplaba estos fines y la protección de los derechos humanos, la nueva propuesta incorpora elementos específicos de derechos humanos en cada uno de ellos, asegurando así un mayor énfasis en su protección desde diversas perspectivas.

Prueba de lo anterior, se destaca que la definición de régimen económico va acorde a los parámetros establecidos por la Asamblea General de las Naciones Unidas y la Organización Internacional del Trabajo respecto de la economía social y solidaria que implica la sostenibilidad social con un empoderamiento sociopolítico de las personas.[\[25\]](#)

Ahora, si bien la definición de Seguridad Nacional incluye las dimensiones personal, comunitaria, salud, alimentaria, económica, ambiental y política de los derechos humanos, elementos que a nivel internacional se estiman como mínimos en las funciones de inteligencia, la Oficina recomienda incorporar directamente el eje de la seguridad humana en esta definición. Este enfoque permitirá optimizar la identificación de factores estructurales que obstaculizan el acceso a derechos humanos y que propician la aparición de condiciones de violencia que impactan directamente en la seguridad nacional. La recomendación de profundizar en la definición surge de la preocupación internacional sobre

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

la necesidad de otorgarle el mayor contenido posible, con el fin de evitar su uso discrecional.[26]

Asimismo, el artículo 3 detalla que se debe tomar en cuenta la competencia civil o militar de los organismos de inteligencia para identificar las causas estructurales que niegan el acceso a derechos y crean las condiciones que atentan contra los fines contemplados. La división clara de competencias de los organismos de inteligencia es clave para evitar su uso indiscriminado, arbitrario o ilegal, ya que asignar funciones de inteligencia a organismos civiles o militares diferentes a su jurisdicción va fuera de los límites de su función y contraviene los derechos humanos. [27] Para garantizar el cumplimiento integral de esta función, ONU Derechos Humanos recomienda que la propuesta de reforma profundice en la regulación de estas competencias, dado que actualmente no existe más normativa que la mencionada en este párrafo.

En el último párrafo del artículo 3, refiere que dichos fines no podrán ser impedimento para articular con los sistemas de rendición de cuentas. Aspecto determinante para delimitar en mayor medida el uso indiscriminado de la inteligencia pues obliga a someter a un escrutinio las actividades de inteligencia para darles validez o remediar afectaciones por su uso arbitrario o ilegal. Este aspecto será desarrollado a mayor profundidad en el punto 3 del concepto técnico.

- 1. Principios que regirán a la inteligencia.** Cómo las labores de la inteligencia y contrainteligencia implican legítimamente actuar con un grado de reserva, es necesario establecer principios que limiten sus actuaciones, garantizando el respeto por los derechos humanos. Estos principios no deben ser reglas rígidas, sino directrices que llenen los vacíos que puedan surgir durante las distintas etapas de la gestión de inteligencia. La propuesta de reforma, en su artículo 5, introduce y desarrolla los principios de legalidad, no discriminación, dignidad humana, necesidad, proporcionalidad, idoneidad, motivación, autodeterminación informativa, rendición de cuentas, oportunidad, gradualidad y distinción. De estos, la ley vigente solo contempla cuatro,[28] por lo que la adición y profundización de los referidos principios representa un avance significativo, especialmente en un contexto de avances tecnológicos que facilitan las labores de inteligencia y requieren alinearse con los estándares internacionales de derechos humanos.[29]

De los referidos principios, la Oficina destaca que el principio de rendición de cuentas haya sido incorporado, pues establece las bases para que se supervise la necesidad, idoneidad y proporcionalidad de las actividades de inteligencia y contrainteligencia para confirmar su validez, suspensión o terminación con su debida reparación si se produjo afectación a los

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

derechos humanos.[30] Como se mencionó previamente, la Oficina profundizará en el principio de rendición de cuentas en el punto 3 del concepto técnico.

Con estrecha interconexión, la incorporación del principio de autodeterminación informativa representa un avance significativo, ya que permite a las personas buscar reparación ante posibles vulneraciones a sus derechos de privacidad y protección de datos personales por el uso arbitrario o ilegal de la inteligencia. Esto es crucial, puesto que las actividades de inteligencia no solo pueden afectar estos derechos, sino también generar condiciones que pongan en riesgo la vida, la integridad personal o provoquen discriminación basada en género, origen racial, étnico o indígena, entre otros.

De acuerdo con los estándares internacionales, la autodeterminación informativa implica que las personas puedan conocer si su información está cumpliendo la finalidad para la que consintió su recolección, a fin de poder objetar su acceso y eliminación en caso de mal uso.[31] Cómo regla general este principio tiene aplicación absoluta con los entes Estatales y privados, sin embargo, para las oficinas de inteligencia existe una limitación válida de como ejercerse.[32] La Oficina seguirá analizando este principio y ofrecerá recomendaciones para su fortalecimiento en el punto 3 del concepto técnico.

Luego, cómo las labores de inteligencia están intrínsecamente relacionadas con el tratamiento de la información con el objetivo de detectar y prevenir amenazas que pongan en riesgo los fines legítimos que buscan proteger, ONU Derechos Humanos resalta que el proyecto de ley incluye un pronunciamiento detallado sobre la aplicación diferenciada de los principios de protección de datos, a saber, la lealtad, minimización, calidad, seguridad de la información y flujo transfronterizo de la información, los cuales son acordes a diversos instrumentos internacionales en materia de protección de datos.[33] Representan uno de los mayores avances en derechos humanos, ya que estos lineamientos aseguran que la información y los datos recabados por las oficinas de inteligencia reciban un tratamiento adecuado en términos de custodia, conservación, acceso y eliminación, garantizando la privacidad de las personas y el manejo adecuado de su información. Esto contribuye de manera significativa a que el resto de los principios y aspectos desarrollados en este concepto tengan efectividad.

Se destaca la incorporación de los principios de flujo transfronterizo de información y supervisión humana suficiente. El primero de ellos porque implica una cooperación internacional con otros Estados y organismos de inteligencia siempre que cuenten con un nivel equivalente de protección de los derechos humanos y protección de datos.[34] Este aspecto es particularmente importante en relación con los estándares actuales sobre el flujo internacional de información, un tema que se abordará en mayor detalle en el punto 6 del

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

concepto.

El segundo principio, relacionado con la supervisión humana suficiente, es fundamental en un contexto de avances tecnológicos, ya que evita que las decisiones se basen únicamente en el análisis de tecnología de procesamiento automático.[35] Garantiza que el uso de tecnologías de vigilancia no reemplace el razonamiento humano en la recolección, análisis y difusión de productos de inteligencia. Los estándares internacionales sugieren que la intervención humana debe ser significativa, como revisar los resultados del procesamiento automático o del perfilamiento,[36] procurando la exactitud de los datos personales para evitar efectos discriminatorios que pongan en riesgo diversos derechos.[37]

En este sentido, la Oficina recomienda que este principio se profundice para que se aplique de manera diferenciada según el tipo de tecnología utilizada, ya que cada una tiene un impacto particular que requiere una intervención humana adecuada.

- 5. Prohibiciones y protección a población históricamente en situación de vulnerabilidad.** El artículo 4 de la propuesta de reforma establece prohibiciones que refuerzan el principio de no discriminación señalado en el artículo 5. Aunque la ley vigente ya contemplaba este principio y solo prohibía involucrar a niños, niñas y adolescentes en actividades de inteligencia, la propuesta actual lo amplía de manera sustancial.

La Oficina destaca la prohibición relativa a que las funciones de inteligencia y contrainteligencia no pueden llevarse a cabo si su objetivo es limitar el ejercicio legítimo de los derechos de reunirse y manifestarse pública y pacíficamente, la libertad de expresión, pensamiento, cátedra y asociación, la defensa de los derechos humanos, la participación en asuntos públicos, la oposición política, el periodismo y la abogacía. Estos aspectos se alinean con los estándares internacionales, como los principios 16 y 17 de los Principios Básicos sobre la Función de los Abogados, el artículo 2 de la Declaración sobre Defensores de Derechos Humanos, y las disposiciones sobre libertad de expresión,[38] y reunión pacífica[39] y de asociación[40] del Pacto Internacional de Derechos Civiles y Políticos. La Oficina recomienda incluir expresamente la función jurisdiccional de jueces y magistrados, dado que, aunque podría estar implícita en lo relativo a la abogacía, su mención explícita evita interpretaciones y sería acorde con los principios 1 y 15 de los Principios Básicos sobre la Independencia de la Judicatura.

Además, el principio de no discriminación, enunciado en el artículo 5, amplía su alcance al señalar que cualquier operación o uso de tecnología no debe basarse en estereotipos o pertenencia a grupos que puedan restringir derechos humanos, ni debe favorecer a ningún

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

grupo por su ideología, opinión política, creencia religiosa, condición social, posición económica u otro factor. Esto constituye un avance importante, ya que incide en garantizar que las acciones sean políticamente neutrales y no favorezcan a ningún grupo.[\[41\]](#) Cualquier diferencia de trato, incluso en la elaboración de perfiles, debe estar respaldada por motivos objetivos y razonables, conforme al derecho internacional de los derechos humanos. [\[42\]](#)

En estrecha relación, también es un avance que la propuesta de ley, en su artículo 7, incluya criterios para identificar las amenazas que habilitan las funciones de inteligencia y contrainteligencia, garantizando que estas acciones no se basen en suposiciones sin fundamento o en criterios automatizados sin supervisión humana. Este aspecto fue destacado por la Corte Interamericana en la sentencia *CAJAR vs. Colombia*.[\[43\]](#)

1. **Educación.** El artículo 6 establece por primera vez en la materia que la formación de agentes y personal de inteligencia debe ser unificado en contenido, con especial énfasis en el conocimiento de derechos humanos para su correcta aplicación. Lo anterior aporta a que los agentes tengan el conocimiento suficiente para identificar cuando una orden conlleva violaciones a los derechos humanos y, consecuentemente, la desobediencia sin miedo a represalias. [\[44\]](#) Para fortalecer dicha formación, la oficina sugiere que el principio de libertad académica sea tomado en cuenta como eje rector de la formación. Éste es esencial para proteger la autonomía de las instituciones académicas y el libre desarrollo de ideas en las aulas.[\[45\]](#)
2. **La adecuación de manuales.** La propuesta de reforma, en su artículo 14 ordena la adecuación de manuales bajo los parámetros que marque la reforma de la ley. Los manuales rigen en cada organismo de inteligencia la correcta aplicación de los principios de inteligencia y protección de datos en cada una de las etapas del ciclo de inteligencia. Por ello, dicha orden generaría que los organismos de inteligencia puedan hacer operacional lo propuesto en la propuesta de reforma; lo que a su vez es ordenado en la sentencia *CAJAR v Colombia* de la Corte Interamericana como medida de no repetición.[\[46\]](#)
3. **Sistema de rendición de cuentas.** El proyecto de ley estatutaria establece diversos controles sobre la función de inteligencia que involucran a varios poderes públicos y a la sociedad civil en labores consultivas, con la dirección de dichos controles a cargo de organismos civiles. Esta modificación refuerza la aplicación del principio de rendición de cuentas y fortalece la legitimidad de las actividades de inteligencia, al contar con mecanismos independientes que garantizan el respeto al Estado de derecho y permiten detectar y reparar violaciones a los derechos humanos en el sistema de inteligencia.[\[47\]](#)

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

4. **Control legislativo.** La Ley de Inteligencia y Contrainteligencia de 2013 creó en el Congreso de la República la Comisión Legal de Seguimiento a las Actividades de Inteligencia y Contrainteligencia, encargada de supervisar políticamente el uso eficiente de los recursos, el respeto de las garantías constitucionales y el cumplimiento de los principios y límites legales para este tipo de actividades. Sin embargo, de acuerdo con los peritajes realizados durante el caso *CAJAR vs. Colombia*, estas funciones no han sido efectivas.[\[48\]](#)

Al respecto, el artículo 29 de la propuesta de ley, amplía las facultades para fortalecer las capacidades de esta Comisión, consistentes en elaborar informes anuales de carácter público sobre el cumplimiento de los objetivos de inteligencia; conocer los objetivos del Plan Nacional de Inteligencia; solicitar al Presidente de la República levantar la reserva total o parcial de información o la desclasificación de la misma por motivos de interés general y cuando exista una base creíble de que se han cometido violaciones a los derechos humanos; presentar oficiosamente denuncias ante las autoridades competentes relativas a abusos, violaciones a derechos humanos o mal manejo de recursos públicos; emitir conceptos sobre el interés de compra y adquisición de tecnologías con fines de vigilancia; realizar auditorías a los organismos de inteligencia para verificar que sus procedimientos vayan acorde a derechos humanos. Para ello podrá articular con el sistema de inteligencia.

La Oficina recomienda que la Comisión podrá articular con expertos en la materia, asegurando decisiones más reflexivas y fundamentadas. Esto se justifica por la necesidad de que los mecanismos de rendición de cuentas posean la suficiente experticia para supervisar eficazmente el sistema de inteligencia.[\[49\]](#)

1. **Órgano consultivo ciudadano.** La normativa propuesta, en su artículo 20, crea por primera vez un órgano consultivo denominado Comisión Civil Ciudadana que constituye un avance significativo en el ejercicio de la democracia participativa. Da facultades a la sociedad civil, en particular a las víctimas, para incidir en los sistemas de rendición de cuentas. Será convocada por la Defensoría del Pueblo, y tendrá facultades de requerir a las inspecciones de las agencias de inteligencia y contrainteligencia las respectivas políticas institucionales de derechos humanos e internacional humanitario, así como requerir a la Comisión Legal de Inteligencia información relativa a sus funciones; además, emitir conceptos por emisiones de ley en materia de inteligencia; conocer y hacer seguimiento de los informes emitidos por el Inspector General de la Comisión de Inteligencia (aspecto analizado en el inciso d en párrafos posteriores); así como recibir un informe anual de las actividades de los Comités de actualización, corrección y retiro de datos.

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

La Oficina recomienda fortalecer las facultades de la Comisión Civil para garantizar un mayor escrutinio de las actividades de inteligencia. Según el derecho internacional, la sociedad civil debe participar en decisiones que contribuyan a la promoción y protección de los derechos humanos.[\[50\]](#) Por ejemplo, el Comité para la Eliminación de la Discriminación Racial en su recomendación general No. 36, ha indicado que el uso de tecnología en la aplicación de la ley sea transparente y permita el examen de la sociedad civil, lo que incluye la participación en la adquisición de tecnologías de vigilancia.[\[51\]](#)

1. **Control judicial.** El artículo 50 de la propuesta de reforma incorpora por primera vez el control judicial para autorizar y supervisar el resultado de ciertas actividades de inteligencia. La autorización previa se necesita cuando impliquen actividades de interceptación de comunicaciones, incluso a través de entidades públicas o privadas, así como aquellas que impliquen la vigilancia de personas. La Oficina destaca que la interceptación de comunicaciones requiere autorización previa, ya que la jurisprudencia internacional establece que, independientemente de la tecnología utilizada para acceder a la intimidad de una persona a través de sus comunicaciones, esto puede constituir una violación al derecho a la privacidad.[\[52\]](#)

Ahora bien, la propuesta de reforma incorpora control judicial posterior siempre que las actividades de inteligencia impliquen la afectación de derechos humanos de personas determinadas o indeterminadas. Al respecto, la Oficina sugiere se sustituyan los términos de “derechos humanos de personas determinadas o indeterminadas” por “derechos humanos derivados del uso de datos sensibles de personas físicas identificables que puedan poner en riesgo su vida privada”. Lo anterior debido a que cierta información de las personas en contextos particulares pueden ocasionar un daño diferenciado si fuera usada de forma incorrecta.[\[53\]](#) Asimismo, la regulación internacional define que una persona física identificable es aquella que puede ser reconocida directa o indirectamente mediante identificadores como nombre, número de identificación, datos de localización, identificador en línea o características físicas, fisiológicas, genéticas, mentales, económicas, culturales o sociales.[\[54\]](#) Dicha recomendación surge de diversas preocupaciones tales como que las mujeres y personas de género diverso son más susceptibles de sufrir abusos, acoso y violencia sexual por el mal uso de información relacionada al libre desarrollo de su sexualidad.[\[55\]](#)

Adicionalmente, ONU Derechos Humanos sugiere que el control posterior profundice su regulación para hacer efectiva la autodeterminación informativa. Esto, pues del escrutinio judicial se podrán identificar datos personales que salen de la finalidad legítima para la que fueron recabadas. En ese sentido las personas afectadas deberán ser notificadas para que puedan disponer de dicha información.[\[56\]](#)

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

1. **Control institucional.** El artículo 18 de la reforma a la ley prevé la creación del Consejo Nacional de Inspectores Generales liderado por la dirección de naturaleza civil (artículo 19), como instancia de coordinación en cuanto a la política institucional para el adecuado control y supervisión de las actividades que realicen los organismos de inteligencia y contrainteligencia.

Se destaca que el rol atribuido al Consejo de Inspectores Generales tiene un impacto significativo para la garantía de los Derechos Humanos en las mencionadas actividades, ya que se le asigna como funciones la adopción de los instrumentos e indicadores de gestión, así como un acuerdo marco con un enfoque en Derechos Humanos, que consagre criterios unificados para desarrollar las actividades de inteligencia y contrainteligencia, y la efectiva supervisión y control de estas.

1. **Procedimiento para la autodeterminación informativa.** El artículo 55 de la propuesta de ley establece el procedimiento a través del cual una persona hace efectiva la autodeterminación informativa para acceder, rectificar o eliminar información personal que no cumpla con los criterios de necesidad, idoneidad y proporcionalidad. Este mecanismo es esencial para garantizar el acceso a la justicia de las personas que sospechen que su privacidad ha sido vulnerada.[\[57\]](#)

La Oficina recomienda ajustar esta regulación conforme a la jurisprudencia internacional, reconociendo que por los objetivos mismos de las actividades de inteligencia, en ciertas circunstancias, el acceso total o parcial a los archivos de inteligencia puede no ser viable.[\[58\]](#) En ese sentido, las autoridades a las que se acudan tienen la responsabilidad de motivar porque no es viable tener acceso a dicha información o, en caso de que los datos ya no cumplan su finalidad para ser almacenada, se garantizará su acceso total o parcial para que la persona afectada determine rectificación y/o eliminación.[\[59\]](#)

En el mismo sentido, la Oficina recomienda profundizar en el escrutinio judicial que pueden tener las decisiones del párrafo anterior. En el sentido que no sólo se combate la negativa al acceso, rectificación o eliminación, sino también se pueden someter al escrutinio judicial decisiones que nieguen tener información de la persona o cualquiera sea la decisión. Para ello, se recuerda que estos mecanismos judiciales deben contar con la experiencia necesaria para acceder a la información de inteligencia y supervisar la necesidad, idoneidad y proporcionalidad de las operaciones, asegurando que no generen discriminación.[\[60\]](#) A partir de ello, se puede confirmar la continuación, suspensión o terminación de cualquier medida de inteligencia.[\[61\]](#) En el entendido que la información reservada será utilizada exclusivamente dentro del marco de los procedimientos destinados a garantizar la autodeterminación informativa, cualquier uso de dicha información fuera de ese marco

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

implicaría la correspondiente responsabilidad para la autoridad judicial.[\[62\]](#)

4. **Uso de la tecnología.** Una diferencia significativa a la ley vigente es la apertura a la adquisición de diferentes tipos de tecnologías, pues en aquella únicamente se permite el uso legal del monitoreo del espectro electromagnético y de acuerdo con la sentencia de CAJAR v Colombia, esta regulación es ambigua y sin un control adecuado.[\[63\]](#) Para ello, la propuesta de reforma contempla varias consideraciones enfocadas en la protección de los derechos fundamentales y el uso responsable de dichas herramientas. Los estándares internacionales reconocen la importancia de las labores de inteligencia y el uso de tecnología es una realidad;[\[64\]](#) por ello, se recomienda poner las medidas necesarias para evitar que éstas violen derechos humanos.[\[65\]](#)

Los principales aspectos relacionados con el uso de la tecnología incluyen:

1. **Tipo de tecnología permitida:** Los artículos 15 y 16 de la propuesta de reforma permiten el uso de tecnologías que faciliten acceder a las comunicaciones mediante la interceptación, recepción, grabación y vigilancia selectiva de cualquier forma de telecomunicación o transferencia de datos a través de medios electrónicos, independientemente del lugar donde esto ocurra, así como softwares o programas para acceder a los dispositivos electrónicos de la persona objeto de esta medida, siempre y cuando haya autorización judicial (ver apartado de control judicial).

Para ello, el artículo 16 establece lineamientos para garantizar el respeto a los derechos humanos: el uso de la tecnología debe motivar con satisfacción los principios de necesidad y proporcionalidad, estar dirigida a fines legítimos, y contar con mecanismos para limitar su alcance intrusivo. Además, se requiere un registro inmodificable de su uso y mecanismos para detener su operación ante sospechas de abuso. La Oficina también recomienda que la tecnología pueda bloquear la información si existe riesgo de fuga.[\[66\]](#)

Estas garantías mínimas son congruentes con los estándares de derechos humanos, así como se articulan con que la autorización del uso de tecnología debe tener aprobación judicial (aspecto desarrollado en el punto 3.c. del concepto), evitando el uso de tecnologías como el malware Pegasus, que no cumple con dichos parámetros según análisis internacionales.[\[67\]](#)

1. **Principios en el uso de la tecnología:** ONU Derechos Humanos saluda que el proyecto de reforma articula de forma adecuada con los principios de derechos humanos que regulan a la inteligencia. En su artículo 15 refiere que la tecnología debe ser utilizada de forma necesaria y proporcional con el fin que se busca proteger; lo

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

cual deberá ser registrado en las órdenes de trabajo de acuerdo con el artículo 13 de la reforma, lo que va en sintonía al principio de calidad de la información que exige el registro para tener información exacta, precisa, completa y actualizada de la gestión de inteligencia. Por último, el artículo 5 introduce el principio de supervisión humana, asegurando que las decisiones tecnológicas puedan ser revisadas para prevenir vulneraciones y garantizar el principio de no discriminación.

2. **Limitaciones en el uso de herramientas de intrusión:** El artículo 4 de la reforma impone prohibiciones para limitar el uso de tecnología en actividades de inteligencia. Se prohíbe el acceso directo a datos, metadatos o comunicaciones sin mediación de los operadores de telecomunicaciones. También se prohíbe la coacción a fabricantes o proveedores de software para que modifiquen sus productos, debilitando la seguridad de las comunicaciones. Esto subraya la importancia del rol de las empresas privadas en el flujo de información y su capacidad de controlar las tecnologías adquiridas.

El inciso l del artículo 4, reafirma la importancia de la intervención humana suficiente, al prohibir autorizar o ejecutar cualquier orden de operaciones o misiones de trabajo basadas únicamente en información o predicciones obtenidas o construidas de forma automatizada.

Además, la reforma de ley también prohíbe la captura, copia o almacenamiento de tráfico masivo de datos, metadatos o comunicaciones generando una vigilancia de forma indiscriminada sin identificar a las personas objeto de las actividades de inteligencia. Al respecto la Oficina recomienda profundizar la regulación y límites de la vigilancia masiva por las siguientes consideraciones:

1. El Alto Comisionado de las Naciones Unidas para los Derechos Humanos advirtió en un reporte que, si bien las tecnologías digitales de procesamiento masivo de datos pueden tener beneficios, su uso por parte de Estados y empresas para la vigilancia intrusiva amenaza con erosionar los derechos humanos al recolectar y analizar grandes volúmenes de información personal, muchas veces sin el conocimiento o consentimiento de los individuos. Esto puede llevar a la manipulación del comportamiento humano, la creación de perfiles detallados y otros abusos si no se implementan controles adecuados.[\[68\]](#) Por ello, se recomienda no utilizar tecnología que no cumpla con los principios de derechos humanos que rigen la inteligencia.[\[69\]](#)
2. Asimismo, en el *Caso Big Brother Watch v Reino Unido*, se establecieron cuatro mínimos para que la interceptación de datos masivos pueda respetar los derechos a la privacidad: 1) autorización judicial previa, 2) información clara a los ciudadanos sobre las condiciones para la interceptación, 3) claridad sobre la selección de comunicaciones para ser examinadas, y 4) mecanismos de control, notificación y recursos efectivos. [\[70\]](#) Además, se identificaron cuatro fases del proceso de

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

interceptación masiva, cada una requiriendo análisis de necesidad y proporcionalidad, bajo supervisión judicial y con recursos efectivos para los afectados.[\[71\]](#)

De forma similar, existen estudios en los que se propone como deben ser los tratamientos de datos derivados de la vigilancia masiva de comunicaciones desde su recopilación hasta su eliminación. Incluye una planeación estratégica, autorización previa, recolección y filtro de la información, procesamiento de datos, análisis de la información, revisión y evaluación, así como su reporte final que podrá ser sujeto de vigilancia.[\[72\]](#)

1. **Adquisición de tecnologías:** La reforma establece prohibiciones específicas en la adquisición de la tecnología, y una regulación que implica un grado de control sobre su adquisición.

Primero, el referido artículo 4 de la reforma, prohíbe la adquisición de tecnología de vigilancia a empresas que estén involucradas en violaciones de derechos humanos o en actividades que no respeten el derecho internacional humanitario; así como tecnología que permita la suplantación de la identidad de las personas (artículo 16 de la propuesta de reforma).

Al respecto la Oficina recomienda que la prohibición añada y considere los Principios Rectores sobre las Empresas y los Derechos Humanos, en el sentido que la negociación con empresas también sea condicionada a que cumplan con sus obligaciones de derechos humanos.

La Oficina reconoce la necesidad e importancia de la referida prohibición de tecnologías que suplanten la identidad, debido a que se limita la adquisición de tecnologías con capacidades como la de Pegasus, la cual una de sus principales características es la manipulación de la información de los dispositivos digitales en los que se instale.[\[73\]](#)

Ahora bien, como se detallará, ONU Derechos Humanos recomienda fortalecer los mecanismos que tengan un control sobre la adquisición de tecnología con las siguientes consideraciones:

En la propuesta de reforma, la Comisión Legal de Inteligencia (artículo 29) es la única facultada para emitir conceptos respecto a la adquisición de tecnología, sin embargo, como se refirió en anteriores párrafos, cada tecnología amerita un escrutinio detallado para vislumbrar sus ventajas, desventajas, y nivel de cumplimiento a los estándares de derechos humanos. Por ello, se sugiere que la adquisición de la tecnología esté aparejada de una evaluación del impacto en la protección de datos. Esta figura es establecida en la normativa

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

internacional de la materia^[74] y actualmente se aplica a tecnologías de procesamiento masivo de la información. La evaluación de impacto describe los posibles riesgos del tratamiento automatizado o la elaboración de perfiles y cómo se puede mitigar. En ese sentido, es viable y razonable hacer una evaluación para la diversidad de herramientas tecnológicas que se puedan adquirir.

Adicional a ello, la Junta de Inteligencia Conjunta -quienes presumiblemente tendrían un mayor grado de experticia en la materia- deberían participar en el escrutinio de la adquisición de la tecnología. Asimismo, se retoma la recomendación que la Comisión Legal pueda articular con expertos en la materia de inteligencia, que incluye el uso de tecnología, pues el análisis de estas evaluaciones implica alcanzar un nivel de tecnicismo adecuado para emitir una opinión acorde a la tecnología.

Fortalecer la adquisición de tecnologías con involucramiento efectivo del sistema de rendición de cuentas fortalece el cumplimiento de los principios de derechos humanos que rigen la inteligencia, cómo lo son que las actividades de inteligencia se sometan escrutinio de los órganos de control, que se pueda determinar la intervención humana suficiente para las herramientas tecnológicas, la protección de datos, necesidad y proporcionalidad, entre otros.

Por último, la oficina reconoce que la propuesta de reforma en su artículo 17 numerales b y c, establece la obligación de realizar un inventario detallado de las tecnologías adquiridas, responsabilizando a los órganos de inteligencia de su uso y garantizando la proporcionalidad de las medidas. Esto fortalecería la protección de datos, asegurando un uso responsable y transparente de las tecnologías.

- 5. Depuración de archivos.** En el Capítulo V del proyecto se establece el Sistema Nacional de Depuración de Datos y Archivos de Inteligencia y Contrainteligencia (SND), cuyo objetivo es garantizar la actualización, corrección y eliminación de estos archivos. Este sistema está compuesto por diversas instancias, entre ellas la Comisión Asesora, la Instancia de Depuración, el Consejo Asesor de Depuración, y los Comités de Actualización, Corrección y Retiro de Datos.

La Instancia de Depuración se crea como una Unidad Administrativa Especial con autonomía administrativa, financiera y presupuestal, encargada de llevar a cabo el proceso de depuración de los archivos de inteligencia y contrainteligencia, en coordinación con cada organismo de inteligencia. Este enfoque responde a recomendaciones y condenas internacionales, en concreto la CEV y la Corte IDH, que han señalado la necesidad de mejorar el manejo de la información. Asimismo, ONU Derechos Humanos reconoce que

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

Comisión Civil tenga incidencia con el SND pues dentro de sus facultades puede requerir un informe anual para comentar su cumplimiento de acuerdo con estándares de derechos humanos (artículo 20 de la propuesta de reforma).

La Oficina recomienda que se busque coordinación para que el Decreto 2149 pueda ser reformado acorde, considerando que también la Corte ordenó su adecuación con base a los estándares internacionales de derechos humanos.

6. Reflexiones adicionales. Una reforma al sistema de inteligencia de Colombia no solo fortalecería la seguridad interna respetando los derechos humanos, sino que también tendría un impacto positivo en las relaciones comerciales, especialmente en el intercambio de información con otros países. Casos recientes, como Schrems I y Schrems II, sirven de antecedente, ya que el Tribunal de Justicia de la Unión Europea determinó que las leyes de inteligencia de EE. UU. no ofrecían suficientes garantías para proteger los derechos fundamentales de los ciudadanos europeos. Esto llevó a la invalidez de los acuerdos comerciales de transferencia de datos entre EE. UU. y la Unión Europea. Algunas de las principales razones detrás de estas decisiones fueron la falta de supervisión efectiva sobre las actividades de inteligencia y la ausencia de mecanismos que permitieran a los ciudadanos europeos defender sus derechos en tribunales estadounidenses.[\[75\]](#)

En este contexto, una reforma en Colombia que incluya una supervisión independiente, mecanismos claros de rendición de cuentas y límites y controles a la vigilancia masiva no solo aseguraría el respeto a los derechos humanos, sino que también mejoraría su reputación como socio comercial confiable. Al adoptar estándares más altos en protección de datos, Colombia facilitaría acuerdos internacionales de transferencia de información, como con la Unión Europea, cuyo enfoque en la protección de datos es riguroso. Esto abriría oportunidades para acceder a mercados más amplios y fortalecer el intercambio de información bajo condiciones de seguridad jurídica tanto para ciudadanos como para empresas de ambos lados.

En conclusión, la aprobación de la reforma en los términos actuales representaría un avance significativo en materia de derechos humanos, al profundizar y clarificar las cuestiones previamente mencionadas. No obstante, la Oficina recomienda incorporar las siguientes precisiones para que la reforma sea más integral y asegure el cumplimiento efectivo de diversas obligaciones en materia de derechos humanos para la gestión de inteligencia.

Resumen recomendaciones:

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

1. **Definición de terrorismo:** Ajustar la definición a la Resolución 1566 del Consejo de Seguridad de la ONU, garantizando que incluya la intencionalidad de causar daño para generar terror, y evitar un uso indiscriminado del término.
2. **Definición seguridad nacional:** Incorporar directamente el eje de seguridad humana para optimizar la detección de factores que niegan el acceso a derechos y generan violencia.
3. **Competencias diferenciadas:** Asegurar una clara distinción entre las competencias de los organismos de inteligencia civil y militar, previniendo el uso indebido de recursos y funciones en actividades que no son de su jurisdicción.
4. **Libertad académica:** Incorporar el principio de libertad académica en la formación de los funcionarios de inteligencia, garantizando que puedan desarrollar pensamiento crítico y entendimiento profundo de los derechos humanos.
5. **Intervención humana en tecnología:** Detallar que la supervisión humana suficiente debe aplicarse de manera diferenciada para cada tecnología, de modo que se adapte a sus características y efectos específicos.
6. **Protección a jueces y magistrados:** Incluir de manera explícita a jueces y magistrados en la protección especial frente a ser objetos de la función de inteligencia de conformidad a lo desarrollado en el punto 1.c del concepto.
7. **Articulación con expertos:** Fortalecer la capacidad de la Comisión Legal de Inteligencia, permitiendo la articulación con expertos externos que puedan aportar conocimientos especializados, especialmente en materia de tecnología y derechos humanos.
8. **Mayor capacidad a la Comisión Civil:** Ampliar las facultades de la Comisión Civil para garantizar un control más robusto y participativo, involucrando a la sociedad civil en los procesos de supervisión, rendición de cuentas y control de actividades de inteligencia.
9. **Control posterior:** Reemplazar los términos «derechos humanos de personas determinadas o indeterminadas» por » derechos humanos derivados del uso de datos sensibles de personas físicas identificables que puedan poner en riesgo su vida privada «, con el fin de precisar y delimitar claramente el alcance del control posterior y garantizar una protección efectiva de la privacidad de las personas.
10. **Capacidad de bloqueo de tecnología:** Asegurar que las tecnologías de vigilancia adquiridas tengan la capacidad de bloquear información si existe un riesgo de fuga, protegiendo la integridad de los datos manejados.
11. **Control sobre adquisición de tecnología:** Establecer mecanismos robustos para controlar la adquisición de tecnologías, asegurando que cumplan con estándares internacionales de derechos humanos y realicen una evaluación de impacto sobre protección de datos.

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

12. **Límites en el comercio de la tecnología:** Adicional a la prohibición de comercializar con empresas con investigaciones por vulneraciones a derechos humanos, añadir que las empresas también deben cumplir con los Principios Rectores sobre las Empresas y los Derechos Humanos.
13. **Autodeterminación informativa:** Matizar la regulación de la autodeterminación informativa conforme a la jurisprudencia internacional de acuerdo con lo detallado en el punto 3.e.
14. **Escrutinio judicial ampliado:** Ampliar el escrutinio judicial sobre las decisiones relacionadas con la autodeterminación informativa, permitiendo que cualquier decisión pueda ser materia de supervisión judicial.
15. **Evaluación detallada de tecnologías:** Realizar una evaluación técnica y de derechos humanos antes de adquirir cualquier tecnología de inteligencia, asegurando que no genere riesgos indebidos para los derechos fundamentales de las personas.
16. **Sistema de Depuración de Archivos:** Asegurarse que el contenido del Decreto 2149 sea congruente con la propuesta de reforma de la ley.

Atentamente

Juliette de Rivero

Representante de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos en Colombia

[1] Comisión de la Verdad en Colombia, 'Hallazgos y Recomendaciones' (2022) 154, 187 and 190.

[2] Comisión para el Esclarecimiento de la Verdad, la Convivencia y la No Repetición, 'Evolución, Funcionamiento y Problemáticas de La Inteligencia Civil y Militar En Colombia (1954-2020)' (2022) 88 y 89.

[3] Comisión de la Verdad en Colombia (n 1) 413.

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

[4] *ibid* 692.

[5] *ibid*.

[6] *ibid* 698.

[7] Comité de Derechos Humanos, ‘Observaciones Finales Sobre El Octavo Informe Periódico de Colombia’ (2023) CCPR/C/COL/CO/8. Párr. 30 y 31

[8] *Carta de alegación 10/2021*.

[9] Alto Comisionado de las Naciones Unidas para los Derechos Humanos, ‘Situación de Derechos Humanos En Colombia’ (2024) A/HRC/55/23 14. Párrafo 72. J.

[10] CIDH. Prácticas de interceptaciones ilegales en Colombia, 177 periodo ordinario de sesiones, 5 de octubre de 2020.

[11] CIDH, Observaciones y recomendaciones - Visita de trabajo a Colombia, junio 2021. https://www.oas.org/es/cidh/informes/pdfs/ObservacionesVisita_cidh_Colombia_spA.pdf

[12] *Caso Miembros de la Corporación Colectivo de Abogados ‘José Alvear Restrepo’ vs Colombia* [671 to 686].

[13] Corte IDH. Caso Colectivo de Abogados “José Alvear Restrepo” vs. Colombia. Sentencia de excepciones preliminares, fondo y reparaciones del 18 de octubre de 2023.

[14] Artículo 68 1. Los Estados Partes en la Convención se comprometen a cumplir la decisión de la Corte en todo caso en que sean partes.

[15] ARTÍCULO 93. Los tratados y convenios internacionales ratificados por el Congreso, que reconocen los derechos humanos y que prohíben su limitación en los estados de excepción, prevalecen en el orden interno. Los derechos y deberes consagrados en esta Carta, se interpretarán de conformidad con los tratados internacionales sobre derechos humanos ratificados por Colombia.

[16] ‘Más detalles sobre la revelación del presidente Gustavo Petro sobre la compra del software espía Pegasus’ *RTVC Sistema de Medios Públicos* (5 September 2024) <<https://www.rtv.gov.co/noticias/denuncia-presidente-gustavo-petro-software-pegasus>> accessed 16 September 2024.

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

[17] W Radio Colombia [@WRadioColombia], '#NoticiaW | @FiscaliaCol inició una investigación para establecer la verdad sobre la denuncia del presidente Gustavo Petro (@petrogustavo), identificar e individualizar a los responsables de la probable adquisición y uso ilegales de software espía "Pegasus" → <https://t.co/JX7NPt5l5F>' <<https://x.com/WRadioColombia/status/1831712932838744396>> accessed 16 September 2024.

[18] El Espectador, "'Dónde está Pegasus': Comisión de Inteligencia y Contrainteligencia del Congreso' *ELESPECTADOR.COM* (16 September 2024) <https://www.elespectador.com/politica/comision-de-inteligencia-da-detalles-sobre-debate-por-software-pegasus-denunciado-por-petro-noticias-politicas/?cx_testId=59&cx_artPos=1&cx_testVariant=cx_1> accessed 16 September 2024.

[19] ONU Derechos Humanos Colombia [@ONUHumanRights], '1/El uso del malware Pegasus vulnera gravemente derechos a la privacidad, libertad de expresión y asociación, entre otros derechos humanos. Las denuncias sobre su compra en 2021 y posible uso deben ser investigados seriamente por las autoridades competentes @FiscaliaCol.' <<https://x.com/ONUHumanRights/status/1831668557400150518>> accessed 2 October 2024; ONU Derechos Humanos Colombia [@ONUHumanRights], '1/ Saludamos que la propuesta de reforma a la ley de inteligencia presentada en el Senado el 4 de septiembre de 2024 contiene mecanismos de control y rendición de cuentas que dificultarían la adquisición de tecnología como el malware pegasus.' <<https://x.com/ONUHumanRights/status/1841123994822377869>> accessed 2 October 2024.

[20] *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 12) para 304.

[21] Comisión de la Verdad en Colombia (n 1) 154, 187 and 190.

[22] The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, 'Compilation of Good Practices on Legal and Institutional Frameworks and Measures That Ensure Respect for Human Rights by Intelligence Agencies While Countering Terrorism, Including on Their Oversight' (2010) A/HRC/14/46 para 9; The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, 'The Role of Intelligence Agencies and Their Oversight in the Fight against Terrorism' (2009) A/HRC/13/37 para 20; *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 12) para 525.

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

- [23] Comisión Interamericana de Derechos Humanos, ‘Corrupción y Derechos Humanos’ (2019) OEA/Ser.L/V/II. Pags. 56 a 60.
- [24] General Assembly, ‘Human Security’ (2024) A/78/665.
- [25] International Labour Organization, ‘Resolution Concerning Decent Work and the Social and Solidarity Economy’ (2022) ILC.110/Resolution II; Asamblea General de las Naciones Unidas, ‘Promoción de La Economía Social y Solidaria Para El Desarrollo Sostenible’ (2023) A/RES/77/281.
- [26] The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 22) para 9; *Caso Miembros de la Corporación Colectivo de Abogados ‘José Alvear Restrepo’ vs Colombia* (n 12) para 532.
- [27] *Szabó and Vissy v Hungary* [2016] European Court of Human Rights Application no. 37138/14 [73].
- [28] La ley vigente contempla no discriminación, necesidad, idoneidad y proporcionalidad.
- [29] *Caso Miembros de la Corporación Colectivo de Abogados ‘José Alvear Restrepo’ vs Colombia* (n 17) pt a.1 to a.5; The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 20) practice 20.
- [30] The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 22). Practices 7,8 and 22.
- [31] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales 2021. Principio 8.
- [32] *Caso Miembros de la Corporación Colectivo de Abogados ‘José Alvear Restrepo’ vs Colombia* (n 12) pt b.3.
- [33] Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales 1990 (Resolución 45/95); Principios Actualizados sobre la Privacidad y la Protección de Datos Personales; Estándares de Protección de Datos Personales para los Estados Iberoamericanos 2016; General Data Protection Regulation 2016; Convenio modernizado del Consejo de Europa para la protección de las personas con respecto al

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

tratamiento de datos personales 2018.

[34] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Principio 11.

[35] General Data Protection Regulation art 22; European Data Protection Board, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018).

[36] European Data Protection Board (n 35).

[37] General Data Protection Regulation. Recital 71.6

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

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

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

[41] The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 22). Para. 18 and 19.

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

[43] *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 12) para 534.

[44] The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 22).

[45] Farida Shaheed, Special Rapporteur on the right to education, 'Academic Freedom' (2024) A/HRC/56/58; Working group on academic freedom, 'Principles for Implementing the Right to Academic Freedom' (2024) A/HRC/56/CRP.2.

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

[46] *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 12). Reparación F9.

[47] General Assembly, 'The Right to Privacy in the Digital Age' (2019) A/RES/73/179. Page 5.

[48] *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 12) para 679.

[49] The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson (n 22). Par. 14.

[50] Human Rights Council, 'Human Rights, Democracy and the Rule of Law' (2012) A/HRC/RES/19/36.

[51] Comité para la Eliminación de la Discriminación Racial, 'Recomendación General Núm. 36 (2020), Relativa a La Prevención y La Lucha Contra La Elaboración de Perfiles Raciales Por Los Agentes Del Orden' (2020) CERD/C/GC/36. Párr. 63.

[52] *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 12) para 543; Office of the United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (Human Rights Council 2022) A/HRC/51/17 para 19.

[53] Principios Actualizados sobre la Privacidad y la Protección de Datos Personales. Principio Nueve.

[54] General Data Protection Regulation art 4.1.

[55] Special Rapporteur on violence against women, and its causes and consequences, 'Online Violence against Women and Girls from a Human Rights Perspective' (2018).

[56] *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 12) para 608.

[57] *CASE OF ROMAN ZAKHAROV v RUSSIA* [2015] European Court of Human Rights, Grand Chamber Application no. 47143/06. Par. 288.

[58] *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 12) para 601.

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

[59] *ibid* 605 and 606.

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

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

[62] *ibid*. Par. 15.

[63] *Caso Miembros de la Corporación Colectivo de Abogados 'José Alvear Restrepo' vs Colombia* (n 12) para 676 a 678.

[64] *ibid* 525.

[65] Office of the United Nations High Commissioner for Human Rights (n 52); General Assembly, 'The Right of Privacy in the Digital Age.' (2020) A/RES/75/176; General Assembly, 'The Right to Privacy in the Digital Age' (n 47).

[66] Fionnuala Ní Aoláin, 'Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach' para 126.

[67] Giovanni SARTOR and Andrea LOREGGIA, 'The Impact of Pegasus on Fundamental Rights and Democratic Processes' (EPRS: European Parliamentary Research Service 2023); Ní Aoláin (n 66).

[68] United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (2018) A/HRC/39/29.

[69] General Assembly, 'The Right to Privacy in the Digital Age' (n 47). Pages 2 and 3.

[70] *CASE OF BIG BROTHER WATCH AND OTHERS v THE UNITED KINGDOM* [2021] European Court of Human Rights, Grand Chamber Applications nos. 58170/13, 62322/14 and 24960/15. Par. 275.

[71] *ibid*. Par. 325 and 350

[72] Thorsten Wetzling and Kilian Vieth, *Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations* (Heinrich-

Concepto técnico de ONU Derechos Humanos sobre la Radicación del Proyecto de Ley Estatutaria No. 225 del 2024 en el Senado por la cual se reforma la Ley 1621 de 2013 (inteligencia y contra inteligencia).

Böll-Stiftung 2018).

[73] SARTOR and LOREGGIA (n 67) 25.

[74] General Data Protection Regulation. Recital 91.

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