Inteligencia y contrainteligencia, ¿violación constitucional?

Autores
Pablo Franco Baquero
Sebastian Osorio Zuluaga

Director
Andrés Palacios Lleras

Derecho

Facultad de jurisprudencia
Economía, sociedad y derecho
Universidad del Rosario

Bogotá - Colombia
2025

Palabras clave

1. Principio de finalidad
2. Orden judicial.
3. Impacto social.
4. Habeas data
5. Estado Social de Derecho
6. Autocensura
7. Regulación.
8. Límites constitucionales.
9. Derechos Humanos
10. Derechos constitucionales.
11. Principio de proporcionalidad

Resumen

Esta investigación se encuentra fundamentada en limitaciones internacionales y nacionales del uso de tecnología de inteligencia y contrainteligencia ante el ciudadano, las limitaciones que este presenta, la regulación nacional e internacional existente y los mecanismos de defensa que existen ante sus abusos.

This research studies the international and national limitations that the use of counterintelligence technologies has on its citizens, what limitations does it present, how its regulated international and nationally and what means of defense does the average citizen count on against the unlawful use of it.

1. Introducción

El primer Estado conocido por la comunidad internacional y los medios de comunicación más prestigiosos en comprar Pegasus fue Israel por allá por el año 2011, a través de la secretaría de defensa nacional. “Pegasus” es un software de espionaje con un hiperdesarrollo tecnológico, que es capaz de sobrepasar los límites de la protección de los datos, y cuyo uso implica la violación de todos los derechos que por conexidad tengan relación con la privacidad, la libertad y el debido proceso de la obtención de información. Este sistema fue desarrollado por la compañía israeli NSO Group, y su enfoque recae sobre la obtención de información personal a través de los dispositivos móviles como celulares, computadores, tablets, etc. Este termina siendo un software diferencial en el mercado ya que puede ser utilizado sin necesidad de que el usuario del dispositivo interactúe directamente con él, lo que quiere decir que no es necesario abrir links, descargar aplicaciones, abrir páginas, ni realizar ningún tipo de acción que, a priori bajo la lógica humana, pueda darle entrada a este software a las fotos, videos, cámara, correos electrónicos, notas y mensajes de cualquier red social o de telecomunicaciones. Esta característica es alarmante ya que su capacidad de infección es totalmente indetectable hasta para los más poderosos sistemas del planeta, es lo que lo hace, por excelencia, el sistema más deseado por todos los Estados del mundo. Precisamente según investigaciones del diario “El Mundo” hay evidencias claras que nos conducen a suponer que este sistema ya ha sido comprado por 45 países a lo largo del globo terráqueo, y se sabe de más de 22 países en donde se descubrieron utilizaciones del sistema a través de instituciones gubernamentales como fiscalías, ministerios, entidades centralizadas y descentralizadas, y hasta empresas particulares del ámbito privado. Las declaraciones de NSO Group son que el sistema fue creado inicialmente con el objetivo de ayudar a los Estados en su lucha contra el terrorismo y el narcotrafico, pero a la hora de la verdad el sistema era vendido sin preguntas ni reproches, teniendo en cuenta que el precio de compra rondaba entre los 12 y los 20 millones de dolares

entre los años 2016 y 2022. Investigadores de la Universidad de Toronto fueron los primeros en descubrir la existencia de una venta de este malware por el año 2016 con la noticia mundial de que era un software de vigilancia común. Un SMS falso fue enviado a Ahmad Mansoor, un activista arabe de los derechos humanos, hecho inicial que condujo al descubrimiento de que la utilización del software no era únicamente con objetivo de ubicar narcotraficantes ni terroristas. Después de este suceso se descubrió que más de 1,400 celulares habían sido interceptados utilizando la aplicación WhatsApp en 2019.

El Estado Colombiano será el principal objeto de esta investigación, en la cual se hará también utilización del derecho comparado para llegar a una conclusión de la incidencia que puede tener Pegasus en el Estado colombiano, su división tripartita y "autónoma" del poder, y las leyes y normas sobre protección de datos, de derechos como la privacidad o el habeas data y el efecto interno e internacional que esto puede significar. En el año 2024 el presidente Gustavo Petro denunció el descubrimiento de la compra del software Pegasus en el gobierno anterior del expresidente Iván Duque, en dicha denuncia se manifiesta que se encontraron pagos de alrededor de 11 millones de dólares en efectivo a la empresa israelí NSO group, desde este suceso se han sumado a las denuncias diversas figuras que conforman el poder legislativo y judicial del país, desde mediados de junio del año 2024 las altas cortes lideradas por el magistrado Jorge Enrique Ibáñez -vicepresidente de la corte constitucional- dieron a conocer que sus equipos y diversos auxiliares de los despachos estarían siendo interceptados. La investigación realizada por el periódico El Espectador indica que:

> *De acuerdo con las denuncias del magistrado Ibáñez, de sus equipos se borró y copió información, razón por la cual, además de dar a conocer públicamente los presuntos hechos, presentaron la información que tenían sobre lo ocurrido ante la*

Fiscalía. Al parecer, manifestaron desde ese despacho, habrían sido víctimas de Pegasus. (...)

Tan pronto como Ibáñez presentó las denuncias, fue respaldado por las altas cortes, quienes pidieron garantías al trabajo de la rama judicial. Según conoció El Espectador, al menos 15 magistrados de la Corte Constitucional, del Consejo de Estado, de la Corte Suprema de Justicia y de la Jurisdicción Especial para la Paz (JEP), declararon ante la Fiscalía y solicitaron que se investigara

De esta manera el problema jurídico que abordaremos en esta investigación consiste en determinar si el Estado Colombiano, con base en la Constitución Política de 1991, los tratados internacionales, la legislación aplicable y las diversas normas relevantes, tiene la facultad de recolectar datos personales de los ciudadanos mediante sistemas como Pegasus, en el marco del ejercicio legítimo de sus funciones y competencias. De igual manera se analizará las implicaciones que tiene la utilización de este mismo sistema para la percepción de las funciones constitucionales y legales del Estado, sus alcances y sus límites en cuanto al régimen interior y exterior que lo regula. Es imperativo analizar de qué manera la división tripartita del poder puede verse afectada si el poder judicial o legislativo es objeto de espionaje y contraespionaje dirigido desde el poder ejecutivo, además de determinar de qué manera los derechos humanos pueden ser también agredidos si no hay mecanismos de defensa efectivos que permitan a las personas protegerse judicial o materialmente de esta medida tan invasiva de la privacidad. En ese sentido también se abordará cuáles son las limitaciones de nuestro marco legal para ejercer un control efectivo sobre esta herramienta y su poder, y sobre todo, si la utilización de dicho elemento implica una pérdida en la seguridad jurídica del Estado, toda vez que las herramientas legales existentes pueden terminar siendo inefectivas en cuanto a su objeto y su efecto.

No es de suponer, de todas formas, que en ejercicio de sus funciones el Gobierno pueda hacer utilización de estas herramientas para asegurar la protección y seguridad del Estado. Es decir que aunque en principio parezca que no hay contexto alguno en el que Pegasus pueda ser utilizado sin transgredir derechos fundamentales, sin afectar la democracias y el Estado social de derecho, o de afectar los principios del derecho y la seguridad jurídica, no se puede suponer que las facultades del Estado para su utilización sean nulas, por lo que también se analizará cuáles son las facultades reales del Estado, y bajo qué contexto el uso de esta herramienta puede estar habilitada en pro del bien común. Lo que lleva directamente a la pregunta de investigación que se ha planteado: ¿El Estado puede, en ejercicio de sus funciones de proteger el orden público, adquirir y usar un software para "capturar" y analizar información protegida por el derecho constitucional de Habeas Data?

2. Regulación Estatal e Internacional.

2.1 Facultades del Estado en inteligencia y contrainteligencia

El Estado colombiano tiene las facultades para realizar actividades de inteligencia y contrainteligencia con el fin de poder salvaguardar aquello que considere puede afectar la seguridad nacional y de sus ciudadanos. Por lo anterior, en la Constitución Política de Colombia, se han establecido 3 artículos de suprema importancia con el fin de que el ciudadano pueda verse protegido ante la implementación de estas facultades en contra del Estado. Basado en esto, se va a realizar un análisis de los artículos 15, 28 y 250; donde se van a exponer las limitaciones institucionales y el mecanismo de protección que puede utilizar el ciudadano en caso de que se vulnere alguno de estos derechos constitucionales. Finalmente, en cuanto a la legislación nacional, se va analizar la ley 1621 de 2013 que tiene por objeto fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y

contrainteligencia; lo anterior en línea con los artículos y principios constitucionales mencionados previamente.

Marco Constitucional frente a la protección de datos Habeas Data

En primer lugar, como fue mencionado previamente, se va a realizar un análisis del artículo 15 de la Constitución, donde se va a explicar porque el *habeas data* se encuentra protegido bajo este artículo y cuál es su alcance frente a la solicitud de información a diferentes entidades dentro del territorio colombiano. Basado en lo anterior, el artículo dicta lo siguiente:

> *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas." (*Constitución Política, 1991*)*

El legislador, al momento de redactar este artículo, encontraba por objetivo otorgarle al ciudadano una base de protección frente a los abusos de poder que pueden emerger por parte del Estado al momento de investigar, donde se debe de tener en cuenta la intimidad y la información que de estos haya sido recolectada por parte de entidades, tanto públicas, como privadas. Este artículo, en cuanto a lo que concierne el *habeas data*, se encuentra perfectamente complementado por el artículo 28 de la Constitución, donde en su primer inciso menciona lo siguiente: *"Toda persona es libre. Nadie puede ser molestado en su persona o familia, ni reducido a prisión o arresto, ni detenido, ni su domicilio registrado, sino en virtud de mandamiento escrito de autoridad judicial competente, con las formalidades legales y por motivo previamente definido en la ley."* (Constitución Política, 1991). La razón por la cual este es de suprema importancia es que da lugar al debido proceso en caso de una investigación judicial en contra de un ciudadano, así dando lugar a las siguientes 3 características de

protección de datos. (1) Garantiza que las entidades estatales no puedan utilizar información en contra de ciudadanos que no haya sido obtenida de manera legal; (2) Garantiza que la información que se encuentre en ordenadores públicos, como pueden ser los antecedentes penales, sean verificados y rectificados a favor del ciudadano; y finalmente (3) Garantiza que el ciudadano no pueda ser detenido por información errónea o manipulada que se encuentre dentro de servidores públicos y privados. Finalmente, en cuanto al marco constitucional, donde se enmarcan los pilares constitucionales frente a la intercepción de comunicaciones y garantías frente a una investigación donde se pueda vulnerar el *habeas data*, es necesario mencionar como el artículo 250 presenta los requisitos y deberes por parte del ente investigativo con el fin de legalizar una posible violación a este derecho.

Para lo anterior, el legislador, dentro del artículo 250 de la Constitución Política, consagra que para poder hacer una intercepción de la información que se encuentra salvaguardada dentro del habeas data, es necesario que se expida una orden judicial por parte de un Juez de Control de Garantías, que en ningún momento puede ser el juez que lleve el proceso. Este artículo menciona que la investigación será llevada a cargo por parte de la Fiscalía General de la Nación y que este ente debe de responderle al ciudadano en caso de que adelante una investigación donde se haya utilizado, parcialmente o en su totalidad, un "software" de vigilancia como PEGASUS, pues estos deben de informar si esta es solicitada por el investigado.

Finalmente, el medio de control que puede utilizar el ciudadano en caso de que el derecho constitucional *Habeas data* sea vulnerado es la **Acción de Tutela**. Esto se debe a que, como se trata de una vulneración a la privacidad e intimidad del ciudadano, y que las consecuencias para aquel que causó el daño puede incurrir en sanciones disciplinarias, administrativas y en casos muy graves, en la intervención de organismos internacionales, hace de este mecanismo el más efectivo para poder subsanar el daño lo antes posible. Por otro lado, este también puede

tener efectos penales como se encuentra tipificado en el Código Penal en su artículo 269F- "Acceso Abusivo a Sistema Informático", donde un ciudadano o trabajador público puede ser investigado si encuentran abuso dentro de sus funciones o que la información que se está recolectando de otro ciudadano o entidad se realiza de manera ilegal o irregular.

Ley 1621 de 2013- Ley de Inteligencia y Contrainteligencia.

La ley 1621 de 2013, denominada como la Ley de Inteligencia y Contrainteligencia de Colombia, tiene por objeto fortalecer el marco jurídico que permite a los organismos cumplir adecuadamente la misión constitucional y legal al momento de realizar actividades de inteligencia y contrainteligencia. El fin de esta es la de establecer los límites y los fines de las actividades de inteligencia y contrainteligencia, cuáles son los principios que los rigen, los mecanismos de control y supervisión, la regulación de las bases de datos, la protección de los agentes, entre otras.

En primer lugar, el artículo 3ro hace referencia a los organismos que se encuentran capacitados para llevar a cabo la función de inteligencia y contrainteligencia en Colombia. Estas son las dependencias de las Fuerzas Militares y Policía Nacional que se encuentren organizar para cumplir con este fin, la Unidad de Información y Análisis Financiero y demás organismos que faculte esta Ley. Ahora bien, la razón por la cual estas entidades son las que explícitamente se encuentran facultadas se debe a que tanto las agencias estatales de protección, como el UIAF, son organismos que buscan la protección del ciudadano y de mantener el órden público.

En segundo lugar, encontramos el artículo más importante de la presente Ley, el artículo 4to: Límites y Fines de la Función de Inteligencia y Contrainteligencia. Este menciona que la acción se encuentra delimitada en su ejercicio por el respeto de los derechos humanos y al cumplimiento taxativo y estricto de la Constitución, la Ley, el Derecho Internacional Humanitario y el Derecho Internacional de los derechos Humanos; específicamente, la función

de inteligencia se encontrará limitada por los principios de reserva legal donde se debe de garantizar la protección del derecho de honra, al buen nombre a la intimidad personal y familiar y finalmente, al debido proceso. Para todo lo anterior, la ley ha tipificado los siguientes tres puntos, con el fin de delimitar los fines de obtención de información para la función de inteligencia y contrainteligencia:

> *"a. Asegurar la consecución de los fines esenciales del Estado, la vigencia del régimen democrático, la integridad territorial, la soberanía, la seguridad y la defensa de la Nación;*
>
> *b. Proteger las instituciones democráticas de la República, así como los derechos de las personas residentes en Colombia y de los ciudadanos colombianos en todo tiempo y lugar –en particular los derechos a la vida y la integridad personal– frente a amenazas tales como el terrorismo el crimen organizado, el narcotráfico, el secuestro, el tráfico de armas, municiones, explosivos y otros materiales relacionados, el lavado de activos, y otras amenazas similares; y*
>
> *c. Proteger los recursos naturales y los intereses económicos de la Nación."*

En tercer lugar, el artículo 5to: "Principios de las Actividades de Inteligencia y Contrainteligencia" menciona que se debe de verificar la relación que puede existir entre la actividad y los fines mencionados previamente, para esto es necesario realizar un **test de proporcionalidad.** Para realizar este "test", es necesario evaluar los siguientes principios. (1) **Principio de necesidad:** Que la actividad de inteligencia y contrainteligencia debe ser necesaria para alcanzar los objetivos y fines constitucionalmente deseados, es decir que para incurrir a ésta no pueden existir otros medios menos lesivos para alcanzar tales fines. (2) **Principios de idoneidad:** Que la actividad utilice medios que se adecuen a los fines determinados previamente, y finalmente, (3) **Principio de proporcionalidad:** Que la actividad

sea proporcional a los fines buscados y que los beneficios del mismo excedan las restricciones impuestas sobre otros principios y valores constitucionales. En síntesis, que los medios y métodos empleados no deben de ser desproporcionados frente a los fines que se buscan encontrar u obtener.

Finalmente, es necesario mencionar el artículo 17 debido a que este es de suprema importancia para el derecho de **hábeas data** ya que fija la finalidad de las intercepciones de las comunicaciones privadas y da lugar a los requisitos que estas deben sobrellevar y los requisitos constitucionales y del Código de Procedimiento Penal. El anterior dispone lo siguiente:

> *"Las actividades de inteligencia y contrainteligencia comprenden actividades de monitoreo del espectro electromagnético debidamente incorporadas dentro de órdenes de operaciones o misiones de trabajo. La información recolectada en el marco del monitoreo del espectro electromagnético en ejercicio de las actividades de inteligencia y contrainteligencia, que no sirva para el cumplimiento de los fines establecidos en la presente Ley, deberá ser destruida y no podrá ser almacenada en las bases de datos de inteligencia y contrainteligencia. El monitoreo no constituye interceptación de comunicaciones.*
>
> *La interceptación de conversaciones privadas telefónicas móviles o fijas, así como de las comunicaciones privadas de datos, deberán someterse a los requisitos establecidos en el artículo 15 de la Constitución y el Código de Procedimiento Penal y sólo podrán llevarse a cabo en el marco de procedimientos judiciales."*

Reglamento General de Protección de Datos de la Unión Europea de 2016

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea entra en vigor en el año 2018, tiene como finalidad el fortalecimiento de la protección de datos y del derecho

universal **habeas data** y otorga a los individuos un mayor control sobre sus derechos personales. Este reglamento se encuentra fundamentado en los principios fundamentales de transparencia, limitación a la finalidad Estatal, la minimización de datos y la limitación del almacenamiento de datos personales y la protección de datos de ubicación.

Para esto, el ente gubernamental en la Unión Europea ha dado en pie a los siguientes derechos individuales, con el fin de que estos sean rectificados. (1) **Derecho de acceso:** Solicitud de información sobre los datos personales que se estén procesando. (2) **Derecho al olvido:** Solicitud de supresión de información y datos personales. (3) **Derecho de rectificación:** Solicitud de corrección y reafirmación a datos inexactos. (4) **Derecho a la portabilidad:** Solicitud de transferir datos de una persona a un segundo responsable. (5) **Derecho a la limitación del tratamiento:** Solicitud a la limitación al uso gubernamental de datos. Ahora bien, en el caso de empresas privadas que se encuentran capacitadas en procesar datos personales, estas deben de seguir una serie de obligaciones como el **consentimiento,** es decir que este debe de ser explícito y verbal con el fin de tratar con datos personales; **la notificación de violaciónes de seguridad** y notificar esta a las autoridades competentes; y finalmente, la **rendición de cuentas** ya que es su deber demostrar que se está cumpliendo con las obligaciones que han sido descritas dentro del Reglamento General de Protección de Datos.

En conclusión, este reglamento ha revolucionado la protección de datos personales dentro de la Unión Europea y América del Sur, ya que permite que los ciudadanos tengan más control sobre sus datos y cuáles son las obligaciones de las entidades, tanto estatales como privadas, en cuanto al manejo, uso y almacenamiento de esa información.

Importancia del sistema de inteligencia y contrainteligencia israeli Pegasus.

El sistema de inteligencia y contrainteligencia Pegasus, creado por la compañía israeli NSO Group, como ya se ha evidenciado previamente, tiene una gran importancia en el mundo

siempre cambiante de la tecnología. Este sistema puede acceder a los dispositivos móviles, bases de datos, entre otros; y de ahí extraer información sensible y de carácter personalísimo justificado por la Seguridad Nacional. Un sistema como este debe de encontrarse regulado por lo entes gubernamentales con el fin de no encontrarse en un área gris donde pueda infringir con el derecho al **habeas data,** para esto, la empresa mencionada anteriormente dicta que únicamente le venden este tipo de tecnología a Estados, mas no a privados, así asegurándose que obedezcan leyes internacionales y nacionales como la ley 1621 de 2013 en Colombia.

Ahora bien, este sistema, especialmente en un Estado que ha tenido varios conflictos internos como es Colombia, es de suprema importancia tener acceso y uso del sistema Pegasus, esto se debe a que la inteligencia que pueden extraer de grupos armados como las disidencias de las Fuerzas Armadas Revolucionarias de Colombia o del ELN puede ser de vital importancia a ponerle fin al mismo conflicto o hacer capturas estratégicas. Por otro lado, este sistema también puede captar mensajes de datos que den lugar a que la inteligencia y contrainteligencia obtenida sea de gran uso para la ciudadanía y protección estatal, así justificando el uso de un sistema como PEGASUS.

Entendiendo los factores positivos que conlleva este sistema, es necesario mencionar de donde pueden nacer las posibles vulneraciones a la seguridad personal y entender que puede haber una incidencia superlativa en cuanto a la protección al derecho constitucional de **habeas data.** Lo anterior se encuentra es fundamental ya que, bajo el uso subjetivo e ilimitado de estas herramientas o con un gran abuso de poder institucional, personas que no han cometido ningún crimen pueden ser susceptibles a que sus móviles, correos, mensajes y otros medios de comunicación sean comprometidos, así causando que información personal se encuentre bajo la disposición de instituciones o personas que no deberían ostentar este nivel de poder en cuanto a inteligencia artificial, marketing, telecomunicaciones, y obtención de la información como

Big Data. A través de este desarrollo las potencias mundiales han sido capaces de desarrollar software y hardware que bien puede considerarse seguro y legal en cuanto a la protección de la privacidad de las personas del común, pero que a la hora de la verdad carece de herramientas que aseguren derechos humanos y fundamentales. Esta premisa será evaluada a través de los criterios que veremos presentados a lo largo de esta investigación, abarcando el marco regulatorio, el derecho comparado, los efectos sociales y políticos y más. Para determinar la importancia de los sistemas de inteligencia y contrainteligencia en el país es necesario hacer un análisis crítico de sus posibles efectos además de sus implicaciones legales.

2.2 Uso de Pegasus sin orden judicial: ¿legalidad o abuso?

En ejercicio de sus funciones para la protección de los intereses generales del Estado las facultades de este mismo están determinadas por marcos legales bien estructurados en cuanto a sus limitaciones y extralimitaciones. En principio, como venimos diciendo desde el inicio de la investigación, nuestro Estado Social de Derecho contempla la existencia de una división tripartita del poder con el objetivo de que cada elemento esencial del Estado se maneje de forma autónoma. Si bien el órgano judicial se supone tiene mera independencia del órgano ejecutivo y legislativo es evidente que tiene que haber una coexistencia e interdisciplinariedad entre dichos órganos para que pueda haber un funcionamiento adecuado del Estado Social de Derecho. En cuanto a la utilización de PEGASUS es evidente que su mera existencia es controversial, y que su utilización, aunque no esté en su totalidad prohibida, se supone que está limitada a un **control previo y posterior**, al igual que cualquier otra herramienta de interceptación de comunicaciones o información. Para asegurarnos de este hecho basta con remitirnos a los precedentes judiciales existentes en el país en cuanto al manejo y la interceptación de información por parte de instituciones como la procuraduría general de la

nación o la fiscalía, y de igual forma podemos citar las leyes y normas existentes que regulan la obtención de información a través de herramientas de espionaje y contraespionaje.

Primeramente, es menester recalcar que este tema tiene un tratamiento marginal en toda la región latinoamericana, tanto en el aspecto básico de la doctrina como en lo legal y organizacional. Legalmente hablando los regímenes existentes proyectan su regulación en relación a los intereses del Estado, más allá de los intereses que puedan tener los gobiernos de turno que utilicen, compren o creen herramientas de contrainteligencia. De igual manera si bien existe la ley 1621 de 2013, se estará analizando su efectividad y eficiencia, al igual que la ambigüedad en su redacción y la imposibilidad del ejercicio efectivo de los elementos que emanan de esta misma. Esto es importante toda vez que no se encontrara realmente ninguna norma específica que regule el procedimiento para el uso de estas herramientas, ni su correcta y específica definición, objeto, alcance o los elementos normativos que deben rodear necesariamente su utilización, aunque sí será más sencillo hablar de aquellas limitaciones que debe tener el espionaje a ese nivel en nuestro sistema democrático.

En Colombia la primera sentencia en materia de privacidad de datos es la **T-414 de 1992**. Esta sentencia es fundamental para el análisis de la evolución de la protección de datos en la medida en que estableció principios fundamentales del **habeas data** en la búsqueda de proteger derechos fundamentales como el **buen nombre, la intimidad o la privacidad**. Precisamente este fue el primer paso en la historia del ordenamiento jurídico colombiano para que existiera el requisito legal de la orden judicial para poder escarbar en la información de las personas y los datos que, se supone, son de único conocimiento del titular de la información y de las instituciones pertinentes. En 1992 el ciudadano Francisco Gabriel Arguelles fue el accionante de esta tutela que eventualmente significaría el realce del debido proceso para la obtención y divulgación de información cualesquiera que sean las situaciones que ameritan la intromisión

del estado en la privacidad de las personas. Si bien en principio la sentencia abarca la información bancaria y los reportes en centrales de riesgo, la realidad es que la sentencia fue un hito en la historia ya que sentaría las bases para las normativas que hoy en día regulan la utilización de herramientas de inteligencia y contrainteligencia. La corte estableció en la mencionada sentencia varios principios jurisprudenciales que serían los argumentos base para la regulación de la obtención de información a través de canales de interceptación de información, y sobre todo que estas acciones estuvieran protegidas y justificadas a través del propio órgano judicial del Estado Social de Derecho. El principio jurisprudencial que más nos interesa para este análisis es el **"principio de finalidad".** Este principio puede verse definido no sólo a través de la doctrina colombiana respecto del **habeas data** y protección de datos, sino que se pudo trasladar a ámbitos comerciales, fiscales y penales. La superintendencia de industria y comercio establece que el principio de finalidad responde directamente a la Constitución y la ley, y existe a la par de un deber de información al respectivo titular de la información que busca obtenerse.

La universidad Externado nos presenta una tesis doctoral que analiza la existencia del principio de finalidad como la base fundamental que determina, incluso, las relaciones comerciales entre Estados. El Estado Colombiano empieza a hacer énfasis en este principio en la medida en que la unión europea lo contempla como el elemento más fundamental para el tratamiento de datos personales de las personas; esto lo podemos ver consagrado en el **RGPD de la Unión Europea**, el cual es considerado a nivel internacional el estándar más alto en materia de protección de datos.

En ese orden de ideas podemos afirmar sin miedo al yerro que la obtención de información a través de herramientas de inteligencia y contrainteligencia es completamente ilegal e inconstitucional de acuerdo con las normas y reglas que se han venido desarrollando al

respecto. Como hemos venido abordando el artículo 15 de la constitución resulta ser el pilar que permite el desarrollo normativo de principios como la **finalidad y de libertad**, y que por encima de todo su existencia se justifica con la protección de derechos fundamentales. De esta forma se puede afirmar que el Estado debe cumplir con el procedimiento legal para la obtención de información y de datos personales; esta es la razón de la existencia del control previo y posterior al que se someten estas actuaciones investigativas. La orden judicial existe no solo para cumplir con requisitos procesales y para cumplir con el deber ser del Estado Social de Derecho, sino que crea una seguridad jurídica alrededor de los elementos que se vienen abordando en la medida en que será un juez de la república quien determine la proporcionalidad de la actuación, si se cumple con el requisito de finalidad y de libertad, y sobre todo si la interceptación es acorde al artículo 15 de la constitución y al avance jurisprudencial que ha tenido Colombia en esta materia. La sentencia **C-594 de 2014** nos permite tener mejor entendimiento de la necesidad de la orden judicial como requisito previo a la interceptación de comunicaciones más allá de su consagración en la ley, si bien el desarrollo de la sentencia es extenso, las consideraciones de la corte indican que:

> "*La interceptación ilegal de comunicaciones es entonces una práctica contraria a los principios democráticos que protegen a los individuos de la arbitrariedad de los agentes estatales. Por ello, la interceptación de comunicaciones, sólo puede ser realizada bajo las condiciones y procedimientos expresamente señalados en la Carta y en la ley, como garantía de los derechos fundamentales, en especial del derecho a la intimidad[68].*"

Esto nos permite identificar igualmente que la interceptación de comunicaciones o la obtención de información de manera ilegal representa entonces una arbitrariedad por parte del Estado. No

solo se habla de que va en contraposición a las normas internas y extraterritoriales más importantes, sino que se estaría transgrediendo la esencia misma del estado democrático.

2.2.1 Casos en los que se ha usado Pegasus y su impacto legal y social.

PEGASUS es una herramienta que lleva en uso más de una década, al menos por lo que se puede saber por la prensa internacional. Su utilización ha sido controversial en la medida en que pareciera que no tiene límites en cuanto a su capacidad de infección y de expansión. Como bien sabemos el primer Estado en comprarlo fue Israel en el año 2011. aunque los casos más mediáticos han sido de países como España, Reino Unido, México y Colombia. Según los reportes de Abc España y The New York Times, México se convirtió en el mayor usuario de este sistema en el año 2018, dando como resultado una interceptación a más de 15.000 números de teléfono celular de forma ilegal. Estas investigaciones también concluyeron que el Estado mexicano fue de los primeros en comprar el sistema de espionaje más peligroso del mundo, pues afirman que: "*Pegasus fue adoptado rápidamente por las autoridades mexicanas, y después de que Enrique Peña Nieto asumiera la presidencia en 2012, dos agencias gubernamentales más lo compraron: la oficina del fiscal general y el CISEN, según funcionarios mexicanos y tres personas que conocen los contratos. (The New York Times, 2022)"* Las críticas no se hicieron esperar ya que hubo una filtración masiva de información interna de estas instituciones a través de la base de datos del ejército que arrojó resultados alarmantes. México ha gastado más de 60 millones de dólares en Pegasus desde su compra y el escándalo ha perseguido al expresidente Enrique Peña Nieto incluso una vez terminado su mandato presidencial.

Por otro lado en Colombia la noticia se hizo pública en el año 2024 después de una denuncia hecha por el mismo Presidente de la República Gustavo Petro, lo que desencadenó a su vez una serie de denuncias hechas por magistrados, trabajadores oficiales del Estado y de las altas cortes

asegurando haber sido víctimas de espionaje e interceptaciones ilegales a través de Pegasus. Una vez hecha la denuncia pública en las redes sociales del presidente, el magistrado Jorge Enrique Ibañez manifestó tener pruebas suficientes para asegurarse a sí mismo víctima de estas interceptaciones ilegales, envió una carta al presidente de la Corte, quien al final fue el encargado de denunciar los hechos para su debida investigación a la fiscal general Luz Adriana Camargo. La información específica que se puede obtener únicamente a través de los reportajes realizados por los medios de comunicación más importantes del país es que Pegasus fue adquirido a mediados del año 2021 y su pago fue realizado en dos consignaciones diferentes a cuentas bancarias anexadas al grupo israelí NSO group en dos fechas distintas. Se afirma que los dueños de la empresa y creadores del software estaban en Colombia en el momento de la consignación de este dinero efectivo en sus cuentas bancarias, lo que dio pie precisamente a la trazabilidad de este dinero y el objeto de la compra.

Para analizar el **impacto legal y social** que tiene esta noticia en nuestro país es necesario entender que el contexto mismo en el que se dio la compra del software era una de las situaciones más delicadas del país en la última década, toda vez que en el año 2021 se dio un estallido social que azotó a Colombia con unas de las protestas más violentas y mediáticas que ha tenido el país en este siglo, dejando un saldo de cientos de personas heridas, decenas de muertos y una división política e institucional en el país que incluso a día de hoy sigue teniendo efectos en la percepción de la población respecto a la política y la seguridad democrática.

El impacto más contundente que tendría el ejercicio de estos actos investigativos de interceptación de comunicaciones a través de pegasus sería en los principios que presentamos anteriormente en esta investigación. El ordenamiento y marco jurídico que hemos establecido está fundado esencialmente en los principios de finalidad y libertad. La intromisión del Estado en la información personal y privilegiada de los ciudadanos implicaría una afectación directa a

la finalidad en la medida en que no existiría argumentación alguna en ninguno de los casos que se ejerza estos actos investigativos; si no existe un control previo que garantice la justificación de tal intromisión en la información delicada de los ciudadanos no existe siquiera un rezago del principio de finalidad. Esto lo podemos afirmar toda vez que la decisión de dicha intromisión queda a merced del subjetivismo de cada trabajador oficial o persona que tenga acceso a la herramienta PEGASUS, es decir que no hay un verdadero control judicial desde el órgano que, en principio, debería ser el encargado del debido uso de esta herramienta en los momentos y contextos adecuados. Esto deja un margen de responsabilidad del Estado en cuanto a violaciones sistemáticas de derechos a la privacidad y a la intimidad. Como hemos recalcado la **Ley 1621 de 2013** es fundamental para entender los límites y alcances de la interceptación de información, pero en cuanto a la **Ley 1581 de 2012** es necesario también afirmar que se estaría transgrediendo en su totalidad teniendo en cuenta que también es un pilar fundamental para el marco jurídico en cuanto a protección de datos personales. La citada ley establece, sobre todo, el **deber de información** que tienen las entidades con los titulares de la información cuando es necesaria la intromisión del Estado en los datos sensibles. Ahora bien, el hecho de que sean disposiciones generales implica que son las primeras normas y disposiciones a las cuales se debe acudir en materia de protección de datos. Esta ley establece los procedimientos básicos para que se pueda dar una intromisión legal del Estado en la información privilegiada; como es de esperarse en dicha ley se contempla el uso de datos privilegiados desde una perspectiva legal en cuanto a la obtención de esta información, pero no se establece el uso de datos que, en principio, fueron obtenidos de una forma ilícita o ilegal. De esta manera la ley regula la forma en la que la información debe ser utilizada y transmitida, pero ya hay una transgresión de los derechos de las personas desde el fondo de la norma si el actuar del Estado reposa en la obtención ilegal de la información. Entonces ¿de qué sirve saber manejar los datos legalmente si no se pueden obtener legalmente? Una vez obtenida la información a través de

herramientas de contrainteligencia resulta descabellado pensar en su utilización legal y acorde a los procedimientos establecidos en ambas leyes citadas. Si de primera mano el Estado no va a asegurar la obtención legal de la información no se puede asumir que la utilización de esta información será procedimentalmente acorde a la ley y al marco jurídico que lo rodea. En ese orden de ideas las acciones contra leyem que vayan en detrimento de la **Ley 1621 de 2013** significará también el desconocimiento de lo establecido en la **Ley 1581 de 201**2, desconociendo a su vez no solo todas las disposiciones generales de obtención de información privilegiada sino también de su utilización, más allá de que el supuesto objeto de la compra de Pegasus sea la lucha contra el narcotráfico y el terrorismo.

En cuanto al impacto social que tendría el desconocimiento de las leyes que existen esencialmente para proteger nuestros datos de una obtención y utilización inconstitucional es evidente que el primer efecto sería la desconfianza legítima en el Estado y en la disposición de nuestra información por parte de las entidades que tienen capacidad investigativa. De este modo podemos dividir los posibles efectos en **1) desprotección e indefensión ciudadana, 2) normalización de la hipervigilancia estatal, 3) crisis de legitimidad del Estado, y 4) Brecha digital y exclusión.**

Primeramente, la desprotección e indefensión ciudadana haría realidad las preocupaciones afirmadas por dejusticia en su informe sobre vigilancia estatal, que viene siendo igualmente lo que venimos desarrollando a lo largo de la investigación:

> "*Más allá de si se hace en el contexto de un proceso judicial o en desarrollo de actividades de inteligencia del Estado, la vigilancia y el monitoreo de las comunicaciones entran en tensión con el derecho fundamental a la intimidad. Tanto así que el artículo 15 de la Constitución plantea la interceptación y el registro de las comunicaciones como una excepción a la intimidad familiar y la privacidad de las*

comunicaciones. No es, sin embargo, el único derecho en juego. El habeas data y la libertad de expresión, la libertad de asociación y la libertad religiosa, entre otros, resultan igualmente comprometidos" (Dejusticia, Cortés Castillo Carlos, Bogotá, Julio de 2014)

De esa manera la ciudadanía entra en un trance legal, no sabe cuándo, como, ni para qué están siendo utilizados sus datos, hasta tal punto de ni siquiera saber qué datos están siendo vigilados por el Estado. Cuando se hace un imaginario sobre la indefensión ciudadana respecto de la protección de datos es fundamental pensar en la ineficacia en la que recaerá el **habeas data**; *el acceso, la rectificación y la cancelación o supresión de la información* privilegiada terminan siendo medidas de control inefectivas, lo que llevaría al ciudadano a apartarse de la misma existencia de este derecho fundamental y de la creencia en su protección sobre el objeto mismo para el que fue creado. Todo esto termina siendo un hilo conductor que nos permite identificar también aquellas medidas de control a gran escala que terminaron siendo inefectivas. Sin la existencia del **habeas data** no podría pensarse siquiera en la capacidad de rendición de cuentas de las autoridades o empresas, dejando el actuar administrativo de este calibre a un descontrol ciudadano total, siendo estos los últimos mecanismos de la ciudadanía en la debida protección de los datos personales en una época hipertecnologica.

Segundo, la normalización de la hipervigilancia estatal normaliza un estatus quo de sospecha constante, lo que quiere decir que el ciudadano tendría que adaptarse a saber que lo están vigilando. En casos de trabajadores oficiales de altas cortes como en Colombia normalizar este hecho puede llevar a fallas estructurales dentro de las mismas entidades estatales. Si bien el primer pensamiento es que se fortalece la transparencia y honestidad, no puede concebirse un mundo donde aquellos que ejercen un poder judicial o institucional de cualquier tipo vivan en una vigilancia y sospecha constante, pues aquellos elementos de la vida privada de cada

persona que no tienen que ver con el ejercicio del poder estarían siendo directamente vulnerados sin una justificación directa. Esto puede tener no solo efectos psicológicos graves sumados ya al nivel de presión que reciben los funcionarios del Estado y de las instituciones más importantes, sino que tendría efectos políticos que podrían ser devastadores en el corto plazo. De esta manera también se puede afirmar que la hipervigilancia estatal tendría efectos en la conducta de los ciudadanos en la medida en que se empiezan a autocensurar y a alterar su conducta por el mismo conocimiento de estar siendo vigilados. La sentencia **C-094 de 2020** aborda este concepto, toda vez que en ella se analiza cómo la presencia de cámaras de vigilancia en vehículos de transporte público puede inhibir a las personas de comportamientos normales y conductas legítimas para evitar dejar registros. De la misma manera un estudio de la *Revista de la Facultad de Derecho de la Pontifica Universidad Bolivariana* aborda cómo la presión, incluso leve, hacia los ciudadanos puede afectar la libertad de expresión, el libre desarrollo de la personalidad y la libertad de prensa (Arboleda, P., Aristizábal, J. (2018). Estudio jurisprudencial constitucional sobre la libertad de expresión y prensa en Colombia: medios de comunicación, censura y autocensura. Revista de la Facultad de Derecho y Ciencias Políticas, 48 (129), pp. 375-400.)

Tercero, una crisis de legitimidad del Estado tiene efecto directo sobre la percepción de la institucionalidad, de los canales democráticos y del orden del Estado. La percepción de impunidad institucional sería la primera de las erosiones en la opinión pública, cuando el Estado puede llevar a cabo cualquier actuar por encima de los derechos constitucionales y fundamentales de la ciudadanía implica que el mismo Estado es delictivo desde su mismo ser, para reforzar un sentido de justicia y de equidad en un Estado Social de Derecho un Estado no puede tener una imagen de impunidad institucional en la medida en que existe el mismo contrato social, la confianza de la ciudadanía está puesta en que el Estado existe para proteger y no para dañar o espiar, si bien es extremista, no es desbordante pensar que si se erosiona el

contrato social sobre el que está fundada nuestra sociedad entonces entramos en un Estado dictatorial, donde se elige quien se vigila y hasta qué punto sin un límite social ni jurídico. De igual manera una hipótesis que contribuye a esta afirmación se establece en la medida en que se pierde el interés de la ciudadanía por acudir a lo canales democráticos formales, es decir que más allá de que la eficiencia y transparencia de las medidas de control entra en conjetura, la realidad social sería que ninguna persona estaría dispuesta a atender a la tutela, las quejas, o la participación ciudadana de ningún tipo, dejando nuevamente al pueblo a merced de un Estado con tal nivel de intervencionismo.

Cuarto, la brecha digital y la exclusión no es más que la limitación de la conducta ciudadana a poner en riesgo todos sus datos personales, cuando la ciudadanía no confía en que sus datos serán utilizados de manera transparente y que no hay un límite real para el nivel de vigilancia a la que pueden ser sometidos entonces los ciudadanos evitan acceder a cualquier tipo de servicios digitales públicos o privados. La cantidad de situaciones hipotéticas que puede suponer un rechazo sistemático de la ciudadanía a la digitalización no es menester, pero esto puede significar una mayor vulnerabilidad de la ciudadanía teniendo en cuenta la disminución de canales de atención, inscripción de proyectos del Estado o promoción de mejoras para cualquiera de las instituciones estatales o de políticas sociales.

2.2.2 Exposición derecho comparado y posturas jurídicas

En cuanto al derecho comparado podemos abordar diferentes posturas jurídicas sobre el uso de inteligencia y contrainteligencia y su marco jurídico. Uno de los aportes investigativos más importantes que enfoca las diversas consideraciones es la *Revista Latinoamericana de Estudios de Seguridad*, (URVIO, Revista Latinoamericana de Estudios de Seguridad No. 26, enero-abril 2020,pp.8-23 ISSN 1390-4299 (en línea) y 1390-3691) en su investigación "*Consideraciones de contrainteligencia en la formulación de estrategias de seguridad: utopía o evolución*

pragmática" escrita por Jaime Castillo Arias. Una de las cosas que es importante recalcar es que en los distintos países de occidente que buscan regular la contrainteligencia el objetivo es evolucionar de lo regional a lo global, es decir que se busca una protección sobre el uso de las herramientas de contrainteligencia con la idea generalizada de que los Estados puedan protegerse entre sí y de otros Estados, pero sobre todo que la normativa que se cree alrededor de este tema sea acorde al derecho internacional, pudiendo jugar en los espacios grises en cuanto a la regulación interna se refiere.

Estados unidos

Por ejemplo, en Estados Unidos la consideración de la contrainteligencia tiene un carácter fundamental. Como sabemos este país es una potencia mundial no solo en lo económico sino también en lo tecnológico e investigativo. Teniendo una de las instituciones más poderosas para interceptar y capturar información Estados Unidos enfoca su marco jurídico de regulación de contrainteligencia en la protección de los intereses del Estado y sus conflictos -sean armados o comerciales- con el resto de países del globo terráqueo. En ese sentido pecan en cuanto a su regulación de carácter interno, puesto que no consideran fundamental su regulación para la protección de derechos individuales de los ciudadanos. En cualquier caso, Michael Van Cleave (2007,2) detalla muy bien el objetivo e importancia de la existencia de la contrainteligencia para Estados Unidos.

> *"En primer lugar, la amenaza de inteligencia extranjera es estratégica, lo que significa que los estados utilizan sus recursos de inteligencia a propósito para obtener ventaja sobre los Estados Unidos y para promover sus intereses. En segundo lugar, las amenazas de inteligencia estratégica no pueden ser derrotadas sólo a través de medidas ad hoc. Las amenazas deben ser contrarrestadas por una respuesta estratégica. Y, en tercer lugar, debe haber un sistema a nivel nacional que integre y*

coordine diversos programas, recursos y actividades para lograr objetivos estratégicos comunes."

De esta manera se puede afirmar que la protección de datos personales y la regulación del uso de las herramientas de contrainteligencia queda subrogado al interés de cada Estado y el objetivo de cada uno para su utilización. No obstante, cabe recalcar que Colombia es uno de los países cuyo conflicto armado interno ha sido más duradero en la historia, llegando a tener diversos grupos subversivos de carácter territorial interno. Esto puede tener un efecto adverso ya que no se enfoca la interceptación de comunicaciones en una estrategia geopolítica o global de defensa de intereses propios, sino que su destino termina siendo la intromisión en la ciudadanía del propio país con el objetivo de acabar con las guerrillas internas y el conflicto armado que lleva azotando al país desde hace más de cinco décadas. Ahora bien, lo que se puede tomar como aprendizaje de Estados Unidos respecto a la regulación de la contrainteligencia son sus propias vivencias históricas. En occidente el país que más regulado tiene este tema es Estados Unidos, no únicamente por su poder legislativo y su capacidad democrática, sino porque ha sido uno de los Estados más afectados por el terrorismo desde la década de los 70. Woods y King (2009, 170) afirman que:

"*Los abusos por parte del FBI, la CIA y los componentes de inteligencia del Departamento de Defensa (DoD) que salieron a la luz a mediados de la década de 1970 condujeron a un amplio marco de ley y regulación destinado a prevenir el uso indebido de los poderes de seguridad nacional."*

sin mencionar que después del atentado terrorista de septiembre de 2001 permitió que se dictara La Ley de Autorización de Inteligencia en el año fiscal 2010. De esta forma Estados Unidos nos lleva una ventaja enorme en cuanto a la regulación de inteligencia y contrainteligencia, no solo en el ámbito regional sino también en el global, teniendo en cuenta que su estrategia de

seguridad la tienen actualizada hasta 2017, tienen una norma legal del Estado expedida desde el congreso, la norma de contrainteligencia esta actualizada hasta 2019, tiene las líneas de acción estratégica definidas específicamente, su ley de inteligencia nacional está establecida desde 1947, y tienen el control legislativo de la materia desde 1970 a través de las dos cámaras del congreso. Para ponerlo en perspectiva para el año 2020 Colombia tenía su norma legal a través del ejecutivo, la estrategia de inteligencia y contrainteligencia estaban únicamente enunciadas, y se creó una comisión especializada de inteligencia en el año 2013, lo que puede perjudicar indirectamente la imparcialidad y transparencia sobre el control efectivo de las normas (información obtenida de *Tabla 1. Estrategias, normativas y control de actividades de inteligencia y contrainteligencia, Consideraciones de contrainteligencia en la formulación de estrategias de seguridad: utopía o evolución pragmática, Jaime Castillo Arias)*

Por su parte la posición de las Naciones Unidas sigue estrictamente ligada a la legalidad de los actos subyacentes a la compra y la utilización de herramientas de espionaje e interceptación de información delicada. La alta comisión de la ONU para los Derechos Humanos se apegó estrictamente y apoyó de manera contundente lo dicho por Michelle Bachelet, quien señaló que "*estos informes confirman la urgente necesidad de regular mejor la venta, transferencia y uso de tecnología de vigilancia y de garantizar una supervisión y autorización estrictas. Sin marcos regulatorios que cumplan con los derechos humanos, existen demasiados riesgos de que se abuse de estas herramientas para intimidar a los críticos y silenciar la disidencia*" (informe ONU, 21 de julio de 2021, derechos humanos). De esta manera la postura social y jurídica de la ONU es que se carece completamente de un marco regulatorio bien adaptado para la existencia de una herramienta de tal calibre. Es menester recordar que la posición de la ONU es imparcial en cuanto a los intereses de cada Estado, pero abogan en su totalidad por la protección de los derechos sociales como la manifestación, el periodismo libre y la libertad de expresión. Precisamente Bachelet también aborda una de las teorías presentadas a lo largo de

esta investigación, ya que agregó que los informes de vigilancia que se dan como resultado de la interceptación de información a través de PEGASUS tiene un efecto psicosocial intenso en el entendido de que las personas empiezan a **autocensurarse** por miedo a la hipervigilancia, lo que en últimas significa que la prensa internacional también puede ser afectada por Estados que tengan tal control sobre la información privilegiada de las personas. Bachelet se dirigió específicamente a Estados Unidos, pues como venimos diciendo este Estado es potencia en esta materia, por lo que se dirige a este país con la intención de recordarles que las medidas de vigilancia solo se justifican en circunstancias definidas rigurosamente. En ese sentido es lógico pensar que dichas manifestaciones van completamente en contraposición al manejo que le está dando Colombia a la utilización y existencia de pegasus dentro del territorio nacional. Más allá de que los primeros afectados han sido trabajadores oficiales de altas cortes del país, y que la preocupación de la ONU va encaminada a la protección de la libertad de prensa y la libertad individual de los voceros de los derechos humanos, la conclusión sigue siendo la misma. Al menos en cuanto a la posición de las Naciones Unidas, Colombia no está ejerciendo un buen uso ni está creando una buena regulación alrededor de la utilización de esta herramienta de espionaje internacional.

2.3 Limitaciones legales y constitucionales

2.3.1 Identificación de los límites impuestos por la Constitución y tratados internacionales sobre derechos humanos

Como lo hemos venido abordando la constitución política de 1991 establece unos límites perfectamente claros. Primeramente, el artículo 15 garantiza el derecho a la intimidad personal y familiar, así como el habeas data, de igual manera se manifiesta que la interceptación de comunicaciones es posible únicamente con una orden judicial. El artículo 28 dice que nadie

puede ser molestado en su persona o domicilio ni privado de su libertad sino con orden de autoridad competente y con las formalidades legales. El artículo 29 garantiza el debido proceso, lo que es aplicable también a investigaciones de inteligencia cuando afectan derechos fundamentales. El artículo 214.2, incluso en estados de excepción, los derechos fundamentales y las garantías deben ser respetados. Estas normas constitucionales marcan perfectamente los límites de las actividades investigativas a las que se hace referencia, como se ha dicho al principio, es más fácil identificar en el marco jurídico colombiano aquellos límites para el uso de herramientas como Pegasus que los procedimientos para su utilización y para la utilización legal de la información obtenida a través de esta herramienta.

Por otro lado, el bloque de constitucionalidad nos permite identificar límites que van por la misma línea legal y jurisprudencial. El pacto internacional de derechos civiles y políticos nos presenta el artículo 17: se prohíben las injerencias arbitrarias en la vida privada o correspondencia; los artículos 9 y 14 exigen la legalidad y el debido proceso que debe llevarse en virtud de las normas internas y territoriales que maneja cada Estado. La convención americana sobre derechos humanos en su artículo 11 el cual protege la honra y la dignidad, el artículo 8 y 9 abarca el debido proceso y la legalidad y el artículo 9 es uno de los que más nos interesa para establecer los límites reales por los posibles efectos de herramientas de vigilancia, puesto que abarca la protección de la libertad de expresión, lo que incluye también la prohibición a la censura indirecta, concepto que ya hemos abarcado como posible efecto psicosocial de la hipervigilancia en los particulares. En cuanto a la Corte Interamericana de Derechos Humano podemos remitirnos al caso Escher y otros vs Brasil, 2009 puesto que establece que cualquier vigilancia estatal debe ser autorizada por una ley clara y precisa, elementos de los que carecen las leyes que regulan la utilización de Pegasus en el territorio nacional; e igualmente establece que debe haber un control judicial efectivo que debe seguir el

principio de proporcionalidad como lo entiende la ONU, cosa que tampoco se puede asegurar a través de una comisión especializada en el ámbito como lo tenemos en Colombia.

Este análisis de los límites que impone la constitución y las normas internacionales a través del **bloque de constitucionalidad** permite que se haga un cuestionamiento serio a otro tipo de derechos que pueden tornarse fundamentales por conexidad si se sigue desarrollando una utilización indebida de herramientas como PEGASUS, que no siguen los límites constitucionales, legales, jurisprudenciales ni los principios más importantes de la doctrina que han venido evolucionando desde hace tres décadas. Pues incluso aunque los límites son claros a través de las normas constitucionales y los derechos fundamentales que no deben ser transgredidos sin debida justificación, aquellos derechos que no son fundamentales pueden adquirir este carácter cuando su afectación puede comprometer otros derechos fundamentales. En ese sentido la hipervigilancia puede afectar el acceso a la información y la libertad de expresión, volviéndose fundamentales por conexidad si el espionaje genera algún tipo de **autocensura**, tal y como lo indican las normas internacionales al respecto. Evidentemente el debido proceso, la salud y la libertad religiosa se tornan del mismo rango, toda vez que las vigilancias masivas pueden vulnerar la privacidad de pacientes o creyentes.

De esta manera se puede identificar toda la línea legal desde el ámbito extraterritorial hasta los derechos fundamentales y las normas constitucionales que generan una barrera inquebrantable que se ve agredida por la mera existencia de PEGASUS en Colombia. La protección reforzada de todos los derechos es suficientemente clara para entender que PEGASUS no está lista para ser utilizada en el Estado colombiano.

2.3.2 Análisis del principio de proporcionalidad y la protección de la privacidad frente a la vigilancia estatal

El principio de proporcionalidad en Colombia está enmarcado por tres elementos clave; *la idoneidad, la necesidad y la proporcionalidad en sentido estricto*. Estos tres elementos son fundamentales en la medida que permiten el desarrollo de actividades que pueden ir en contraposición a los derechos fundamentales de las personas sin necesidad de transgredirlos en su totalidad. Fueron creados para poder impartir justicia en aquellos casos donde es necesaria la intromisión o la violación de derechos fundamentales para poder asegurar decisiones justas, trasparentes y acordes a la ley. El objetivo es determinar que aunque haya ciertas acciones, sean investigativas, decisorias o de cualquier índole, que puedan afectar derechos fundamentales de las personas, existe un grado de necesidad, de daño y de falta de medios distintos para poder asegurar la imposición de la justicia en los casos en los que se requiera.

La idoneidad

La corte suprema define la idoneidad de esta manera "*toda intervención de los derechos fundamentales debe ser idónea para contribuir a alcanzar un fin constitucional legítimo*", en principio es evidente que no debería definirse la idoneidad con el mismo concepto de lo que es idóneo, pero la realidad es que este mismo principio se autodefine en la medida en que su existencia exige que la medida que sea adoptada sea la más adecuada para alcanzar el fin legítimo que se persigue. En el contexto de la vigilancia estatal esto implica que la herramienta debe ser utilizada precisamente para lo que fue creada y no para fines que pueden llegar a ser ilegítimos, es decir que la idoneidad de la utilización de PEGASUS recae en que su utilización sea encaminada a prevenir, investigar y luchar contra el terrorismo y el narcotráfico. En ese sentido cualquier otro fin para el que sea utilizado PEGASUS puede considerarse ilegítimo.

Necesidad

En cuanto al principio de necesidad su desarrollo doctrinario y jurisprudencial en Colombia se ha visto permeado especialmente por el ámbito penal. *La Revista de Pensamiento Penal* y la

sentencia **C-365 de 2012** establecen este principio como una especie de desarrollo de **subsidiariedad**. En ese sentido se refiere a que cualquier medida coercitiva, punitiva o que afecte derecho de particulares y que sea ejercida por parte del Estado debe ser la última opción, que además debe ser ejercida sólo cuando no se encuentren alternativas distintas para alcanzar el fin legítimo, lo que implica necesariamente que antes de llegar al ejercicio de un acción que puede afectar derechos constitucionales debe buscarse alternativas distintas que puedan llegar al mismo fin legítimo sin la lesividad que puede representar la última de las opciones. Dado que herramientas como PEGASUS permiten un acceso total a todo tipo de información de las personas sin que los usuarios puedan llegar a tener el más mínimo conocimiento al respecto, resulta obvio entender que existen muchas más formas de llegar a un fin legítimo sin ese nivel de intromisión por parte del Estado, y aunque fuera la última de las opciones resulta totalmente contrario al principio de necesidad que dicha intromisión se haga de manera ilegal e ignorando el deber de información que tiene el Estado hacia los particulares para hacerles saber qué tipo de información será recolectada y cuál será el objetivo por el que se hará ese nivel de intromisión. En cualquier caso en la lucha contra el narcotráfico y el terrorismo no significa esto que deba informársele a las personas objeto de investigación que serán investigadas, puesto que en el ámbito penal no se requiere el ejercicio de este deber de información, no obstante, si se requiere que un juez analice detalladamente el tipo de información será interceptada y cuál es el fin legitimo para el cual será utilizada esta información, cosa que no puede ser posible sin el control judicial pertinente.

Proporcionalidad en sentido estricto

Más conocida como la "**ponderación**" en Colombia la proporcionalidad en sentido estricto requiere un análisis detallado de los derechos que serán vulnerados y las medidas que se van a tomar en pro del objetivo por el cual se restringirán estos derechos. En ese sentido se busca que

haya un equilibrio entre el **daño** realizado y la **ganancia** que se obtiene de la intromisión del Estado en derechos fundamentales y constitucionales. Para casos como el de PEGASUS definir estos límites es complejo toda vez que en un país azotado por la violencia y el narcotráfico las medidas más desesperadas pueden resultar las más adecuadas para acabar con el problema. Si el objetivo legítimo es identificar plenamente narcotraficantes, cabecillas o terroristas, la intromisión en la información privada resulta justificable, el problema puede recaer en los efectos adversos que puede tener esta hipervigilancia en las personas que no son reconocidas ni identificadas como ninguno de estos actores delictivos. Es decir, los efectos colaterales que tiene investigar conversaciones, correos, cámaras, videos y fotos para las personas que no incurren en ningún actuar que justifique esta violación de derechos constitucionales.

De igual manera se debe analizar si el objetivo realmente puede ser alcanzado a través de estas medidas de vigilancia. Para este análisis la sentencia **C-406-2022** es fundamental ya que analiza si realmente hay un efecto en la disminución de la delincuencia cuando se somete a la ciudadanía a una hipervigilancia constante, concluyendo así si realmente someter a los particulares a una vigilancia desmedida afectando su libertad y privacidad puede significar una ganancia en la paz de la ciudadanía y el uso de espacios públicos sin riesgos de delincuencia. Las conclusiones de la corte son que no hay una correlación efectiva entre estos dos factores:

> "*Varias de las investigaciones realizadas sobre este tema han encontrado poca correlación entre la cantidad de circuitos cerrados de vigilancia y seguridad y el crimen o la seguridad. Por ejemplo, la ciudad de Taiyuan, en China, la primera en la lista con una prevalencia de 119,57 cámaras por cada 1.000 habitantes tiene un índice de delincuencia de 51,47%. "En términos generales, más cámaras no necesariamente reducen las tasas de criminalidad". Este dato no solo es importante para cuestionar la relación entre la*

vigilancia y la seguridad. Esta información le interesa a la Corte Constitucional, porque afecta la evaluación de la necesidad e idoneidad de la medida objeto de control en el marco del juicio de proporcionalidad propuesto. En este sentido, confirma también los hallazgos hechos por la Corporación en decisiones anteriores."

Por lo que no se puede suponer en el caso de PEGASUS que someter a los particulares a una vigilancia constante de sus acciones puede tener un efecto positivo en la disminución del narcotráfico y el terrorismo, y mucho menos se puede asumir que la interceptación ilegal a altos funcionarios o particulares tendrá ningún efecto en la lucha contra el narcotráfico y el terrorismo en Colombia.

2.4. Mecanismos de defensa del ciudadano y rectificación de datos recopilados ilegalmente.

Los mecanismos de defensa que pueda utilizar el ciudadano en el Estado colombiano son de suprema importancia ya que estos permiten que, una vez se hayan vulnerado derecho constitucional, como el de **habeas data, la intimidad o al debido proceso,** se pueda solicitar información con el fin de poder corroborar que efectivamente a este se le está o no investigando y subsecuentemente poder tomar una acción con el fin de que se rectifique este error. Para lo anterior, es necesario seguir una serie de pasos ante el **Estado** con los mecanismos constitucionales consagrados dentro de la Constitución Política de Colombia.

En primer lugar, se debe presentar un **derecho de petición** ante una de las siguientes entidades estatales: (1). Fiscalía General de la Nación, (2). Policía Nacional, (3). Dirección Nacional de Inteligencia. Ante estos, es necesario pedir, de manera escrita o verbal, que se le informe al individuo si éste es o ha sido objeto de actividades de vigilancia o seguimiento digital por parte

de la Entidad. Ahora bien, el hecho de que este sea solicitado implica que el ciudadano también debe de explicar la razón por la cual se presenta sospecha de que sus dispositivos digitales han sido intervenidos por una o varias entidades estatales. Finalmente, la autoridad cuenta con 15 días hábiles para realizar la contestación del derecho de petición.

En segundo lugar, se puede interponer una **acción de tutela** ya que se ha presentado una vulneración a uno o varios de los 3 posibles derechos constitucionales mencionados previamente. Esta debe de ser impuesta ante cualquier juez de la República y subsecuentemente será enviado ante un juez competente que hará manejo del proceso y dará una resolución en primera instancia. En caso de que el fallo no sea a favor del ciudadano o no se dé el resultado esperado, éste podrá interponer el recurso de **impugnación** donde un superior jerárquico revisará la petición y así dará una resolución al proceso jurídico.

Por otro lado, y frente a la recopilación de datos personales que fueron adquiridos de manera ilegal, la ley 1581 de 2012 y el Decreto 1377 de 2013 permiten al ciudadano **conocer** qué datos se tiene sobre un individuo, saber cómo estos fueron recopilados y actualizar o rectificar los datos que sean incorrectos o desactualizados. Ante la situación presentada previamente, y que se evidencia alguno de los casos, se puede solicitar la eliminación de esta información ante la entidad pertinente mediante un derecho de petición o una queja ante la entidad.

Finalmente, el ciudadano consternado con que se ha violado alguno de sus derechos constitucionales, puede acudir a una Organización No Gubernamental (ONG) con el fin de que estos lo puedan asesorar sobre qué hacer frente a esta situación, realizar un estudio forense del dispositivo que se crea ha sido vulnerado y hasta ayudar con los costos legales del proceso ante el Estado colombiano. Algunas de las organizaciones que operan en Colombia son la Fundación Karisma, Dejusticia y la Fundación para la Libertad de Prensa.

2.4.1. El rol de los organismos internacionales frente a la protección de los derechos constitucionales frente al uso de sistemas de inteligencia en contra de sus ciudadanos.

El uso de los sistemas de inteligencia y contrainteligencia como Pegasus ha generado preocupación a nivel internacional debido a que este incide una violación a los derechos humanos. Ante la problemática presentada anteriormente, varias organizaciones han creado un sector dentro de la misma con el fin de investigar y revelar qué Estado o privados han utilizado indebidamente un software espía como el de Pegasus. Las empresas que han creado esta iniciativa de transparencia y denuncia son, entre otras, Amnistía Internacional, Human Rights Watch, Citizen Lab International, etc. Todas y cada una de ellas de suprema importancia ya que llevan a cargo la laboriosa tarea de investigar y documentar los casos en los que se confirma que se ha utilizado un sistema de inteligencia abusivo frente a periodistas, defensores de derechos humanos, líderes opositores en países con conflictos internos y más al punto, evidenciando como el sistema Pegasus no está siendo utilizado con la finalidad que propone la empresa NSO Group de utilizarlos para combatir el terrorismo, así causando alarma a nivel internacional.

Gracias a la claridad que han otorgado estas empresas privadas frente a la falta de regulación y el uso abusivo e indebido de este sistema, la Organización de las Naciones Unidas, dentro de sus relatorías especiales ha condenado explícita y públicamente el uso de software espías con fines represivos, más específico cuando se trata de personas de especial protección como los mencionados previamente y así han solicitado dentro de los marcos legales institucionales se dé lugar a que estos sean adecuados con el fin de proteger los derechos fundamentales de todas las personas, más aún, aquellos individuos de especial protección. Por otro lado, en casos de que se dé uso de estos, se debe de garantizar que estas herramientas sean utilizadas bajo el

estándar del **test de proporcionalidad** que ha sido discutido y mencionado a lo largo de este paper de investigación.

Finalmente, el sector privado también cuenta con un rol de responsabilidad frente a la finalización o limitación del uso de estos ya que empresas como Apple, Google, Meta también son responsables de recolectar datos de los individuos que compran y consumen sus productos y, posteriormente, vender esa información con fines desconocidos. Ante esta problemática, diferentes Organizaciones No Gubernamentales han iniciado lo que se podría denominar como "litigios estratégicos" en contra de empresas privadas con el fin de que diferentes tribunales europeos encuentren responsables por los flagrantes abusos al derecho de habeas data, debido proceso y más.

3. Conclusión

Finalmente, en este punto final, se realizará una síntesis de los hallazgos presentados dentro de todo este trabajo formativo y posteriormente, se dará respuesta a la pregunta de investigación y las razones por las cuales el uso de los sistemas de espionaje es incompatible con la carta política de Colombia.

En primer lugar, la implementación de un sistema de inteligencia y contrainteligencia como Pegasus sin orden judicial **viola** los derechos fundamentales, en específico el del debido proceso, privacidad y libertad; y, por otro lado, la violación al derecho constitucional de habeas data. Ahora bien, es importante mencionar que, aunque este tipo de sistema es adquirido con el fin de combatir contra el terrorismo, o por lo menos asi es como lo comercializa la empresa israelí NSO Group, el Estado colombiano ha regulado su implementación en caso de tener que utilizarlo con otros fines. El marco legal en lo que concierne esta investigación se encuentra en la Ley 1581 de 2012, Ley 1621 de 2013, Ley 1266 de 2008 y la Constitución Política de Colombia, donde, como se ha podido evidenciar en repetidas ocasiones, se hace su mayor

esfuerzo para que se puedan proteger los derechos de los individuos, pero que al final del día, dejan varias lagunas legales para que el mismo Estado, y aquellos que pueden utilizar este sistema, lo utilicen de manera indiscriminada y sin orden judicial, así vulnerando los derechos fundamentales y constitucionales de los cuales es poseedor el ciudadano colombiano. Por otro lado, en el esquema internacional, tanto en latino américa como en Europa, se ha dado lugar a una iniciativa solicitando mayor regulación debido a que, en un planeta que cada vez más utiliza la tecnología y los medios de comunicación, es necesario se protejan los derechos fundamentales que fueron mencionados previamente ya que estos se encuentran en constante vulneración por individuos o Estados que tienen agendas contrarias a salvaguardar a la población general y que utilizan los sistemas de inteligencia para beneficio personal.

Por otro lado, y respondiendo a la pregunta de investigación propuesta previamente, podemos concluir que la implementación de un sistema de inteligencia y contrainteligencia como Pegasus sin orden judicial es **incompatible** con el Estado de derecho. Lo anterior se debe a que en Colombia existe una regulación normativa y una multitud de tratados internacionales de la cual hacemos parte, establece los casos en concreto en los cuales se puede interceptar y capturar datos personales sin que se viole el derecho constitucional de **hábeas data,** y los derechos fundamentales del **debido proceso, privacidad y libertad** sin que antes se formule una orden judicial previa. Gracias a esto, podemos concluir que el uso arbitrario de Pegasus o sus sistemas equivalentes sin algún tipo de regulación clara y delimitante pueden causar un abuso de poder y varias violaciones a diferentes derechos humanos, por lo que siempre primará el ordenamiento judicial ya que, sin este, la implementación del mismo irá en contra del Estado de Derecho.

4. Bibliografía

Congreso de Colombia. (1991). Constitución Política de Colombia. Recuperado de https://www.corteconstitucional.gov.co/inicio/constitucion/

Congreso de Colombia. (2012). Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de Colombia. (2013). Ley 1621 de 2013: Por la cual se expide el Estatuto de Inteligencia y Contrainteligencia. Diario Oficial No. 48.771. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52653

Congreso de Colombia. (2008). Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data para el manejo de la información contenida en bases de datos personales. Diario Oficial No. 47.219. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34306

Congreso de Colombia. (2000). Ley 599 de 2000: Código Penal Colombiano. Diario Oficial No. 44.097. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Corte Constitucional de Colombia. (1992). Sentencia T-414 de 1992. M.P. Ciro Angarita Barón. Recuperado de https://www.corteconstitucional.gov.co/relatoria/

Corte Constitucional de Colombia. (2011). Sentencia C-748 de 2011. M.P. Jorge Iván Palacio Palacio. Recuperado de https://www.corteconstitucional.gov.co/relatoria/

Corte Constitucional de Colombia. (2012). Sentencia C-540 de 2012. M.P. Nilson Pinilla Pinilla. Recuperado de https://www.corteconstitucional.gov.co/relatoria/

Corte Constitucional de Colombia. (2013). Sentencia C-913 de 2013. M.P. Jorge Iván Palacio Palacio. Recuperado de https://www.corteconstitucional.gov.co/relatoria/

Superintendencia de Industria y Comercio (SIC). (s.f.). Delegatura para la Protección de Datos Personales. Recuperado de https://www.sic.gov.co

Amnistía Internacional. (2021). Informe técnico: Pegasus Project. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Citizen Lab. (2021). NSO Group's Pegasus spyware: Analysis and findings. Munk School of Global Affairs & Public Policy, University of Toronto. https://citizenlab.ca/2021/07/project-pegasus/

Consejo de Europa. (2022). Human Rights and the Use of Spyware Technologies: Committee on Legal Affairs and Human Rights. https://www.coe.int/en/web/commissioner/view/-/asset_publisher/ugj3i6qSEkhZ/content/spyware-and-human-rights

Human Rights Watch. (2022). "So We Know Who to Target": Government Use of Pegasus Spyware to Surveil Journalists and Activists. https://www.hrw.org/report/2022/02/01/so-we-know-who-target/government-use-pegasus-spyware-surveil-journalists-and

Naciones Unidas (ONU). (2021, julio 12). UN experts call for global moratorium on sale of surveillance technology. Office of the High Commissioner for Human Rights (OHCHR).

https://www.ohchr.org/en/press-releases/2021/07/un-experts-call-global-moratorium-sale-surveillance-technology

Tribunal Europeo de Derechos Humanos. (2018). Case of Centrum för Rättvisa v. Sweden (Application no. 35252/08). https://hudoc.echr.coe.int/

Apple Inc. (2021). Apple sues NSO Group to curb the abuse of state-sponsored spyware. https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

Counterintelligence Considerations in the Formulation of Security Strategies: Utopia or Pragmatic Evolution. Jaime Castillo Arias. 2020. Revista latinoamericana de estudios de seguridad, https://www.researchgate.net/publication/339394235_Consideraciones_de_contrainteligencia_en_la_formulacion_de_estrategias_de_seguridad_utopia_o_evolucion_pragmatica_Counterintelligence_Considerations_in_the_Formulation_of_Security_Strategies_Utopia_or

Consideraciones sobre la inteligencia en la experiencia internacional. Juan Pablo Jarufe Bader. Enero 2023, biblioteca del congreso nacional de chile /BCN, https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/33948/1/Consideraciones_sobre_inteligencia_en_la_experiencia_internacional.pdf

Principios y recomendaciones preliminares sobre la protección de datos. Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos. Consejo permanente de la organización de los estados americanos, comisión de asuntos políticos. Octubre 2011, https://www.oas.org/es/sla/ddi/docs/CP-CAJP-2921-10_rev1_corr1.pdf

Privacy Act, Estados Unidos. FBI, freedom of information. 1974

Carpenter V.s US. The right to keep personal data private, 2018, https://www.bing.com/ck/a?!&&p=beacb8b9bac3d8e37d122eb9774113d0dd5802e2a5775104a4c56c8ab0bd129fJmltdHM9MTc0NjMxNjgwMA&ptn=3&ver=2&hsh=4&fclid=1c3995b0-80e9-61dc-0204-861581fb60bb&u=a1aHR0cHM6Ly9ibG9nLmNvdW5zZWxzdGFjay5jb20vY2FycGVudGVyLXYtdXMtbGFuZG1hcmstc3VwcmVtZS1jb3VydC1ydWxpbmctb24tZGlnaXRhbC1wcml2YWN5Lw&ntb=1

The US legal system on data protectionin the field of law enforcement. Safeguards, rights and remedies for EU citizens. Prof. Francesca Bignami, George Washington University Law School, Washington, DC, USA. 2015. European Parlament. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2705618

The Data protection act United Kingdom. 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents#:~:text=Data%20Protection%20Act%202018%20is%20up%20to%20date,data%204.%20Processing%20to%20which%20this%20Part%20applies

The Doctrine of Confidential Information and Privacy in United Kingdom and Sri Lanka. 2021. https://www.researchgate.net/publication/376359640_The_Doctrine_of_Confidential_Information_and_Privacy_in_United_Kingdom_and_Sri_Lanka

Arboleda, P., Aristizábal, J. (2018). Estudio jurisprudencial constitucional sobre la libertad de expresión y prensa en Colombia: medios de comunicación, censura y autocensura. Revista de la Facultad de Derecho y Ciencias Políticas, 48 (129), pp. 375-400.

Corte suprema de justicia de la nación. Ponderación entre derechos fundamentales. https://www.scjn.gob.mx/sites/default/files/transparencia/documentos/becarios/195carmen-vergara-lopez.pdf

Corte Constitucional de Colombia. (2022). Sentencia C-406 de 2022. M.P. Cristina Pardo Schlesinger. recuperado de https://www.ambitojuridico.com/sites/default/files/2023-03/Sent-C-406-22.pdf

Corte Constitucional de Colombia. (2014). Sentencia C-594 de 2014. M.P. Jorge Ignacio Prelelt Chaljub. C-594/14 Corte Constitucional de Colombia

Reglamento General de Protección de Datos de la Unión Europea de 2016. https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Corte Constitucional de Colombia. (2020). Sentencia C-094 de 2020. M.P. Alejandro Linares Cantillo. recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=137850

Corte Constitucional de Colombia. (2012). Sentencia C-365 de 2012. M.P. Jorge Ignacio Pretelt Chaljub. recuperado de_https://www.corteconstitucional.gov.co/relatoria/2012/c-365-12.htm

Corte Constitucional de Colombia. (2022). Sentencia C- 406 de 2022. M.P. Cristina Pardo Schlesinger. recuperado de http://www.secretariasenado.gov.co/senado/basedoc/c-406_2022.html