La protección de datos personales frente a los sistemas de vídeo vigilancia en Colombia.

Edward Andrés Beltrán López

Universidad La Gran Colombia

Facultad de Derecho

Bogotá D.C.

2.016

La protección de datos personales frente a los sistemas de vídeo vigilancia en Colombia.

Edward Andrés Beltrán López

Código: 6000812014

Email: andresbeltran1010@hotmail.com

Universidad La Gran Colombia

Programa Derecho

Bogotá D.C.

2016

Tabla de Contenido

Cuadros y gráficos

Resumen

La sociedad Colombiana ha permitido la instalación masiva de cámaras de vigilancia, ubicándolas en cualquier establecimiento público o privado, como por ejemplo: bancos, supermercados, autobuses, colegios, trabajos, conjuntos residenciales, entre otros. Dicha instalación ha permitido a los propietarios de los bancos de datos, desconocer el derecho que tienen todos los ciudadanos en proteger, garantizar y autodeterminar sus datos personales, por ello, guiare la discusión en resolver el siguiente escenario constitucional: ¿Hay violación del Derecho a la protección de datos personales (artículo 15. C.P.) cuando cámaras de vídeo vigilancia recaban datos personales sin autorización del titular en Colombia?. A fin de identificar la importancia que tiene la autorización -conocida jurisprudencialmente como la autodeterminación informática- como aspecto medular para el tratamiento de datos sensibles por las cámaras de vídeo vigilancia en Colombia.

La problemática planteada se aborda, desde una metodología cualitativa, es decir, el examen y el análisis se logra luego de la recolección de información y jurisprudencia relacionada con el problema planteado, utilizando como referente metodológico la técnica desarrollada por el profesor Diego López Medina en lo que él denomina como análisis dinámico y estático del precedente.

Como resultado de la metodología planteada, se obtuvo que a lo largo de los años se ha mantenido una línea jurisprudencial bien definida, la cual reconoce que para poder realizar el tratamiento de datos personales de categoría sensibles -biométricos-, es indispensable la autorización del titular.

Concluyendo que si no existe una autorización libre, previa y expresa o exceptuada mediante un expreso mandato legal o una orden de una autoridad judicial, estamos en frente de la lesión directa al Derecho de la protección de datos personales, por lo que tenemos que remitirnos a la acción de tutela o a los mecanismos establecidos en la Ley Estatutaria No 1581 de 2012 frente a la Super Intendencia de Industria y Comercio, Delegatura de datos personales.

Palabras Clave

Autorización, Autodeterminación Informática, Cualificación, Datos Personales, Datos Biométricos, Habeas Data, Sensible,Tratamiento, Vídeo vigilancia.

Abstract

Colombian society has allowed the massive installation of surveillance cameras, placing them in any public or private establishments, such as banks, supermarkets, buses, schools, jobs, housing complexes, among others. This installation has allowed owners of databanks, ignoring the right of all citizens to protect, secure and self-determine your personal data, therefore, shall guide the discussion on solving the following constitutional scenario: Are there any violation of the right to the protection of personal data (Article 15 CP) when video surveillance cameras collect personal data without the authorization in Colombia ? To identify the importance of jurisprudencialmente authorization, known as the Informática- self-determination as key aspect for the processing of sensitive data by video surveillance cameras in Colombia.

The issues raised are addressed, from a qualitative methodology, ie, examination and analysis is achieved after gathering information and jurisprudence related to the problem, using as methodological reference the technique developed by Professor Diego López Medina in he calls the previous dynamic and static analysis.

As a result of the proposed methodology, it was found that over the years has maintained a well-defined line of case law which recognizes that in order to perform the processing of personal data -biométricos- sensitive category is indispensable authorization of the owner .

Concluding that if there is no free, prior express or excepted authorization by an express legal mandate or an order of a judicial authority, are in front of direct injury to the law of the protection of personal data, so we have to use tutela or the mechanisms established

under the Statute Law No 1581 of 2012 compared to the Super Administration of Industry and Commerce, Delegatura of personal data.

Keywords

Authorization, Informative Self-Determination, Skills, Personal Data, Biometrics, Habeas Data, Sensitive, Treatment, Videovigilancia.

Introducción

Para comenzar con la presente exposición, es importante traer a referencia los diversos instrumentos internacionales, tales como: La declaración Universal de los derechos humanos, el convenio para la protección de los derechos y las libertades fundamentales, el pacto internacional de derechos civiles y políticos, y la convención americana de derechos humanos, que reconocen el derecho de toda persona a su vida privada y familiar, y otros instrumentos como la resolución 509 (Consejo Europeo, 1968) y la resolución 3384 de la (ONU, 1975) que reconocen los beneficios y logros que tienen los desarrollos científicos y técnicos en los Estados, donde se pacto con el Estado, la obligación de tomar medidas que extiendan los beneficios de la tecnología a la población y a su vez, ser garante en la protección de las posibles consecuencias negativas que se desprendan por el uso indebido de la tecnología, respetando la vida privada, la persona humana y su integridad física.

El concepto de protección de datos personales no surge inmediatamente y tampoco se encontraba catalogado como Derecho fundamental, fue gracias a entidades como el Consejo de Europa, La Organización de las Naciones Unidas, La Organización para la Cooperación y Desarrollo Económico por sus siglas en inglés (OECD) y el Parlamento Europeo, que a partir de 1970 se comenzó a pronunciar sobre determinados requisitos para ejercer tratamiento de información a la luz del Derecho Fundamental de la Intimidad. Directrices como la (OECD, 1980) y el Convenio 108 del Consejo Europa buscan proteger los datos de carácter personal, frente al tratamiento de datos por medios informáticos o “automatizados”, ya que esta automatización facilita la circulación o flujo transfronterizo de información.

La famosa obra literaria de George Orwell, llamada “1984” considerada como ciencia ficción, logra plasmar una sociedad como la actual, en donde sus ciudadanos no tienen privacidad e intimidad, es esa sociedad digital que oye, ve, recolecta, procesa y analiza todo la información que sus ciudadanos entregan indiscriminadamente; es la transformación de las costumbres físicas a las digitales, permitiendo monitorizar y controlar los cambios que se realizan en ella, es decir, todas las decisiones que se tomen en la sociedad irán atadas a la captura de información que tome el omnipresente diseñando nuestro futuro. La “telepantalla” como la describe Orwell es la que recibe y transmite la información “simultáneamente. “Cualquier sonido que se hiciera… superior a un susurro, es captado por el aparato. Además, mientras se permanece dentro del radio de visión de la placa de metal, podía ser visto a la vez que oído.” (Orwell, 1949).

Por lo tanto se plantea la siguiente pregunta problemática de carácter investigativo: ¿Hay violación del Derecho a la protección de datos personales (artículo 15. C.P.) cuando cámaras de vídeo vigilancia recaban datos personales sin autorización del titular en Colombia? Teniendo en cuenta, el escenario constitucional de la autorización como situación fáctica y medular para el tratamiento de información personal.

Por consiguiente, se inicia respaldando la afirmación que, de acuerdo a la jurisprudencia de la Corte Constitucional, lo establecido en la Constitución Política, la Ley Estatutaria No. 1.581 de 2.012 y sus decretos reglamentarios, la autorización o la autodeterminación informática es considerada como el “pilar fundamental del habeas data,” la cual debe ser libre, previa y expresa o exceptuada mediante un expreso mandato legal o mediante una orden de una autoridad judicial y sin ella se lesiona en directo el Derecho Fundamental a la Protección de Datos Personales.

Por ello, los propietarios de los sistemas de vigilancia – responsables de la información- deberán adherirse a la Ley Estatutaria No. 1581 de 2012, es decir, deberán garantizar que los titulares de manera expresa autoricen el tratamiento de los datos biométricos.

En este sentido, es necesario analizar desde la teoría de los Derechos Fundamentales el Derecho Fundamental a la Protección de Datos Personales y su relación vinculante con el tratamiento de imágenes por parte de los sistemas de vídeo vigilancia. Para ello, en primera instancia, se observará el concepto y la autonomía del Derecho Fundamental al Habeas Data desde enfoque de optimización de principio de Robert Alexy.

Con el objetivo general de identificar la importancia que tiene la autorización -conocida jurisprudencialmente como la autodeterminación informática- como aspecto medular para el tratamiento de datos sensibles por las cámaras de vídeo vigilancia en Colombia.

Lo anterior se encuentra en marcado bajo la línea de investigación propuesta por la Facultad de Derecho de la Universidad La Gran Colombia denominada: *Derecho y sociedad.*

La problemática planteada, se aborda bajo una metodología de investigación cualitativa, es decir, el examen y análisis que se logra luego de la recolección de datos, para obtener información relacionada con el problema planteado. Así mismo se tendrá como referente metodológico para el análisis de sentencia el desarrollado por el profesor Diego Eduardo López Medina en lo que denomina análisis dinámico y estático del precedente. Los cuales pretenden mostrarnos la posición de la corte constitucional en el desarrollo del supuesto fáctico de la autorización en el tratamiento de datos personales en Colombia.

De igual forma**,** los instrumentos metodológicos que se utilizaran como doctrina: Libros, revistas, artículos científicos y jurisprudencia, con el fin de dar respuesta sobre la obligatoriedad de la autorización en el tratamiento de datos personales de categoría sensibles.

En consideración a lo anterior, en primera instancia se desarrollará la conceptualización del Derecho Fundamental a la Protección de Datos Personales, realizando un análisis dinámico y estático de la jurisprudencia de la Corte Constitucional de acuerdo al escenario constitucional de la autorización como situación fáctica propuesto.

En segunda instancia, se identificaran los principios que gobiernan la autorización en el tratamiento de datos personales, basándonos el la optimización de principios como enfoque en la garantía constitucional de los mismos.

En la tercera instancia, se definirá que es un dato sensible, luego se clasificará en dato biométrico, sus clases y características, el cual se encuentra estipulado en la Ley Estatutaria No. 1581 de 2012, decretos reglamentarios y sentencia C-748 de 2011.

En la cuarta instancia, identificaremos los sujetos que intervienen en el tratamiento de datos personales, conociendo los roles que se derivan de los sistemas de vídeo vigilancia.

Finalmente nos referiremos a los sistemas de vídeo vigilancia, con la finalidad de conocer e ilustrar los tipos de cámaras y los sistemas aplicables, pudiendo ser estos análogos o digitales.

El Derecho a la Protección de Datos Personales en Colombia

En el año 1983 y tomando el concepto de (López, M. 2012) un "sitio de producción" como Alemania, País sajón, con la sentencia del Tribunal Constitucional, dio vida a un nuevo concepto llamado "autodeterminación informativa o informática." definida como señala (Remolina, 2013, pág. 28) "La autodeterminación comprende la triada compuesta por la persona, sus datos personales y sus derechos constitucionales." Es la facultad que tiene el titular del dato de poder decidir sobre sus datos personales.

Pero, **¿Qué es el Derecho a la Protección de Datos Personales?** Para definir que es el derecho a la protección de datos personales, tomare como base a (Remolina, 2013) donde cita que nuestra asamblea constituyente, tras varios debates e iniciativas, propuso términos como "libertad Informática, hábeas data[1], datos personales, tratamiento, avances tecnológicos, base de datos, banco de datos, informática y la intimidad", que no lograron su vinculación directa con el texto constitucional, pero que años posteriores nuestra honorable Corte Constitucional los incluyo como Principios y Reglas Constitucionales que posteriormente veremos; por ahora se definirá como el Derecho que tiene toda persona de decidir y conocer sobre sus datos personales, saber quién es el responsable, encargado, que tipo de tratamiento se práctica, quienes tienen acceso a los datos, conocer las medidas de seguridad aplicables, señalar las condiciones actuales y futuras del procesamiento de la información, y en general los principios que gobiernan la regulación. Entonces **¿Qué se entiende por dato personal?** Según lo define la Ley Estatutaria 1.581 de 2.012, un dato

[1] Sobre el origen de la denominación "hábeas data" señala Bazan que "se utiliza a modo de empréstito terminológico tomado del hábeas corpus. Recordamos que este significa ´que tengas el cuerpo (ante el juez) ´; en el caso del hábeas data se quiere connotar ´que tengas (o traigas) los datos´. Como se cita en Remolina, (2013).

personal es “Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.” (Colombia, 2012)

Otra definición es la entregada por el profesor Ernesto Lleras y señalada por el M.P. Dr Ciro Angarita en la sentencia base T-424 de 1992 de la Corte Constitucional:

> “El dato que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, es de su propiedad, en el sentido de que tendría ciertos derechos sobre su uso. Datos de este tipo serían sus señales particulares, relaciones de propiedad y de familia, aspectos de su personalidad, y señales de identidad de diversa índole que van emergiendo en las actividades de la vida. Todos estos datos combinados en un modelo, son equivalentes a una "huella digital" porque el individuo es identificable a través de ellos.” (Colombia, Corte Constitucional 1992)

Por su parte, la sentencia C 748 de 2011 de la Corte Constitucional, en su considerando 2.5.6.1. reitero cuales son las características que hacen a un dato personal y señalo:

> *“i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación.* (Colombia, Corte Constitucional 2011)

Si dato personal significa lo anteriormente señalado, pasemos entonces a definir **¿Qué se entiende por tratamiento?** Conforme lo establece la Ley Estatutaria No. 1.581 de 2.012, el tratamiento es "cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión." (Colombia, 2012)

Ahora veamos, **¿Qué es una base de datos?** de acuerdo a la Ley Estatutaria No. 1581 de 2012 en su artículo 3º numeral segundo expresa: "Base de datos: Conjunto organizado de datos personales que sea objeto de Tratamiento" (Colombia, 2012); y con base a la sentencia C-748 de 2011, las bases de datos cobijan "todo espacio donde se haga alguna forma de tratamiento del dato, desde su simple recolección, lo que permite extender la protección del habeas data a todo tipo de hipótesis."(Colombia, Corte Constitucional 2011)

En consonancia con lo anterior, se puede señalar que los sistemas de vídeo vigilancia al captar **-tratamiento-** la imagen de una persona, puede identificarla a ella y solo ella **-dato personal-** y dicha información se puede almacenar en una **base de datos.** Por consiguiente que el Derecho a la Protección de Datos Personales es vinculante con los sistemas de vídeo vigilancia dado que se cumple los 2 supuestos principales: Dato y Tratamiento.

Conceptualización derecho fundamental

En relación a (Alexy, 2014, p. 34), bajo la dimensión analítica del derecho, la norma es entendida como "el significado de un enunciado normativo" pero entonces **¿Qué se entiende por enunciado normativo?** Este es entendido como el artículo positivo que contiene una norma. Para el caso que nos atañe veamos como ejemplo:

Enunciado normativo: *"**Artículo 6°. Tratamiento de datos sensibles.** Se prohíbe el Tratamiento de datos sensibles, excepto cuando: a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización;…"*(Colombia, 2012). Así las cosas, la norma que se sustrae será: Se prohibe el tratamiento de datos sensibles a menos que el titular haya dado su autorización explicita.

Teniendo en cuenta el concepto de norma y la de enunciados normativos, es necesario conceptualizar que es un Derecho Fundamental. Para ello tomaremos como referencia a (Alexy, 2014) y nos plantearemos la pregunta en concreto **¿Cuáles normas de una constitución son normas de Derecho Fundamental?** Son "Las disposiciones de derecho fundamental pueden ser divididas en dos grupos siendo **(i)** las directamente estatuidas por la constitución -precisión- y **(ii)** las normas adscritas de derecho fundamental" (p. 50) es decir, frente al primer grupo, se puede inferir que en referente a la normativa colombiana son las contenidas en el Título II Capítulo I, artículos 11 al 41 de la Constitución Política, allí es donde encontramos el siguiente disposición de derecho fundamental que reza:

> "**Artículo 15.** 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 los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser

> interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley." (Colombia, 1991)

De modo que, para el segundo grupo -las adscritas- se opta por lo estipulado por (Alexy, 2014, p. 53) que dice, que estas "son aquellas que la jurisprudencia y la ciencia del derecho realmente adscriben a las de precisión." El ejemplo de una norma fundamenta de adscripción es el reconocimiento como Derecho Fundamental a la Protección de Datos Personales, el cual para ser valido jurídicamente, necesita de una "*correcta fundamentación."*

Para cumplir con dicha fundamentación y en atención a (Alexy 2014, p. 262) una forma de hacerlo, es utilizando el precedente Constitucional, ya que el *"uso del precedente supone también una contribución a la seguridad jurídica y a la protección de la confianza den la aplicación del Derecho"* Además que se deben seguir las siguientes reglas:

- *"Cuando pueda citarse un precedente en favor o en contra de una decisión debe hacerse,*
- *Quién quiera apartarse de un precedente, asume la carga de argumentación."* (Alexy, 2014. p. 265)

En consecuencia con lo anterior y con la técnica propuesta por el Dr. Diego Medina, correspondiente al análisis dinámico y estático del precedente, inicialmente, se señalara la evolución del Derecho a la Protección de Datos Personales, luego se hará énfasis en su

autonomía y categoría como derecho fundamental, todo esto bajo el supuesto fáctico de la autorización, que es relevante para el desarrollo del escenario constitucional descrito.

Análisis dinámico jurisprudencial de la autorización desde 1992 hasta 2015.

Para poder desarrollar un buen análisis dinámico jurisprudencial (Lopez, 2006), se planteo un escenario constitucional, el cual se identifica en base al patrón fáctico del caso; para el nuestro se consideró el siguiente: ¿Hay violación del Derecho a la protección de datos personales (artículo 15. C.P.) cuando cámaras de vídeo vigilancia recaban datos personales sin autorización del titular?

Desde el año 1.992 y por medio de la sentencia T-414 de 1992 del M.P. Ciro Angarita[2], con base a (Remolina, 2013) introdujo el término "autodeterminación informativa" a través del concepto de "libertad informática", entendido como:

> Consiste la libertad informática en la facultad de disponer de la información, de preservar la propia identidad informática, es decir, de permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás. (Subrayado fuera del texto). (Colombia, 1992)

En referencia a la sentencia base y a lo largo de los años (1992 – 2015), nuestra honorable Corte Constitucional ha desarrollado un lineamiento jurisprudencial acerca de la

[2] Padre del Derecho a la protección de datos en Colombia. Primer magistrado de la Corte Constitucional que a sus sentencias le atribuía cláusulas de obligatoriedad, conforme a la autonomía que tiene esta alta corte, Tomado de: (López, M. 2006).

autodeterminación informática -la autorización del titular del dato- veamos lo que señala la sentencia T-022:

> "Como sujetos a quienes le concierne la información, los titulares de los datos tienen los derechos que le reconocen la Constitución Política y la ley, particularmente los de acceso, certificación, rectificación y cancelación. De todo lo anterior... se infiere que son idóneos para identificar a su titular y afectar eventualmente su libertad, dignidad, honor y honra. Este riesgo -propio y característico del dato personal- explica en buena medida la exigencia de que su circulación y uso haya de estar necesariamente precedida por formal y expresa autorización de su titular, la cual, adquiere la entidad de una manifestación escrita." (Colombia, Corte Constitucional, 1993)

La Corte por medio de está sentencia hace un llamado a la doctrina constitucional[3] integradora[4], señalando que en caso de un enfrentamiento entre la intimidad en sentido amplio y el derecho a la información "… esta sala no vacila en reconocer que la prevalencia del derecho a la intimidad sobre el derecho a la información, es consecuencia necesaria de la consagración de la dignidad humana como principio fundamental y valor esencial a la vez del Estado social de derecho en que se ha transformado hoy Colombia, por virtud de lo dispuesto en el artículo primero de la Carta de 1991." (Colombia, Corte Constitucional, 1993)

> En efecto, la intimidad es, como lo hemos señalado, elemento esencial de la personalidad y como tal tiene una conexión inescindible con la dignidad humana. En

[3] Entiéndase esta como: Es el nombre como se designan las interpretaciones que hace la Corte Constitucional de la Constitución y las leyes, con ocasión del ejercicio de sus competencias mediante autos y sentencias. Véase: (Quinche, 2014)

[4] "Consiste en las interpretaciones de la Constitución y de la ley hechas por la Corte Constitucional, que tiene carácter obligatorio, en atención a que se trata de la aplicación con autoridad de la Constitución." Véase: (Quinche, 2014)

> consecuencia, ontológicamente es parte esencial del ser humano. Sólo puede ser objeto de limitaciones en guarda de un verdadero interés general que responda a los presupuestos establecidos, por el artículo 1o. de la Constitución. No basta, pues, con la simple y genérica proclamación de su necesidad: es necesario que ella responda a los principios y valores fundamentales de la nueva Constitución entre los cuales, como es sabido, aparecen en primer término el respeto a la dignidad humana (Corte Constitucional, 1993).

Parafraseando Remolina (2.013), es evidente, como la Corte Constitucional y magistrados de tan alta talla como lo era el Dr. Ciro Angaria Barón, veían la necesidad de garantizar esta universalidad comprendida como el derecho a la Intimidad. Hasta el año 1.995 y por medio de la sentencia SU-082 de 1995 del M.P. Dr. Jorge Arango Mejía, nace otra línea interpretativa que ha sobrevivido hasta la fecha, la cual ubica al Derecho de Protección de Datos como un Derecho Autónomo, y se pregunta la Corte ¿Cuál es el núcleo esencial del habeas data? A juicio de ella, está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial económica. (Colombia, Corte Constitucional 1995)

Asimismo, esta sentencia hito[5], se aclaró que el consentimiento tiene tres cualificaciones que son libre, previo y expreso, y que del consentimiento se desprende los derechos y deberes de los recolectores de datos personales; es decir, que la "Autorización debe ser expresa y voluntaria por parte del interesado, para que sea realmente eficaz, pues de

---

[5] Entendido este como *"Son aquéllas en las que la Corte trata de definir con autoridad una subregla de derecho constitucional más complejo que el que en un comienzo fue planteado por las sentencias fundadoras de línea."* (López, 2006)

lo contrario no podría hablarse de que el titular de la información hizo uso efectivo de su derecho."(Colombia, Corte Constitucional 1995)

No fue sino hasta en la sentencia T-729 de 2002 del M.P. Dr. Eduardo Montealegre Lynett, que en su ratio decidendi[6] reafirma:

Bajo el principio de Libertad, "los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo y expreso del titular, de tal forma que se encuentra prohibida la obtención y divulgación de los mismos de manera ilícita (ya sea sin la previa autorización del titular o en ausencia de mandato legal o judicial). En este sentido por ejemplo, se encuentra prohibida su enajenación o cesión por cualquier tipo contractual." (Colombia, Corte Constitucional 2002)

Esta ratio decidendi, fue de nuevo reiterada en sentencia T-310 de 2003 por medio de la M.P. Dra. Clara Inés Vargas Hernández.

En el año 2003 y en la sentencia C-431 del M.P. Dr. Alfredo Beltrán Sierra, se exceptúa por primera vez la autorización del titular del dato en el supuesto fáctico que solo se puede grabar a un ciudadano, en espacios públicos bajo una orden judicial emitida por un fiscal, cuando se quiera impedir la ejecución o consumación de conductas punibles y bajo los siguientes límites:

> (i) que estas actividades no pueden quedar al capricho o al arbitrio de quienes desempeñen funciones de policía judicial, por lo cual se requiere de la existencia de circunstancias objetivas externas que constituyan indicios concretos sobre el particular o la existencia de a lo menos un principio de prueba. (ii) En segundo lugar,

[6] Entiéndase esta como un enunciado concreto, contenido en la sentencia, que define el caso o el pleito, mediante la formulación de una regla cuya aplicación genera la decisión o el resuelve del caso concreto; (Quinche, 2014).

> se estableció que las actividades de incursión o seguimiento deben realizarse exclusivamente para la identificación, individualización o captura posterior, cuando se cumplan para el efecto los requisitos constitucionales o legales, o para impedir la ejecución o consumación de conductas punibles. (iii) En tercer lugar, se exigió que la decisión se motive expresamente para facilitar el control preventivo de las conductas delictuosas y garantizar el derecho a no ser molestado ni individualmente ni en su familia cuando no existan los motivos previstos por la ley para el efecto. (iv) Finalmente se contempló que las actividades de incursión o seguimiento pasivo deben ser temporales y realizadas de manera razonable: "Adicionalmente, se observa por la Corte que las actividades de incursión o seguimiento pasivo a que se refiere la disposición acusada no pueden ser de carácter permanente e indefinido, sino que necesariamente habrán de ser temporales y realizadas de manera razonable, de tal suerte que en ningún caso puedan significar hostigamientos abusivos, pues la política criminal del Estado ha de adelantarse siempre conforme a la Constitución. (Colombia, Corte Constitucional, 2003)

Seguidamente, en la sentencia C 748 de 2011 precedente hito se señala que:

"el tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento." (Colombia, Corte Constitucional 2011)

Sentada esta afirmación, la Ley E. No. 1581 de 2012, en su artículo 3° nos define la AUTORIZACIÓN como el "Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales." Y en su artículo 9° reza "Sin perjuicio de las

excepciones previstas en la ley, en el tratamiento se requiere la autorización previa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser de consulta posterior"(Colombia, 2012) la Corte siendo más precisa en la sentencia aclara totalmente que "no está permitido el consentimiento tácito del Titular del dato. El consentimiento que brinde la persona debe ser definido como una indicación específica e informada, libremente emitida, de su acuerdo con el procesamiento de sus datos personales." (Colombia, Corte Constitucional 2011)

> No está permitido el consentimiento tácito del Titular del dato y sólo podrá prescindirse de él por expreso mandato legal o por orden de autoridad judicial, **(ii)** el consentimiento que brinde la persona debe ser definido como una indicación específica e informada, libremente emitida, de su acuerdo con el procesamiento de sus datos personales. Por ello, el silencio del Titular nunca podría inferirse como autorización del uso de su información (Colombia, Corte Constitucional 2011)

Sin embargo en el artículo 10º de la Ley E. 1581 de 2012 el legislador fue explícito en determinar las excepciones a esta regla las cuales son:

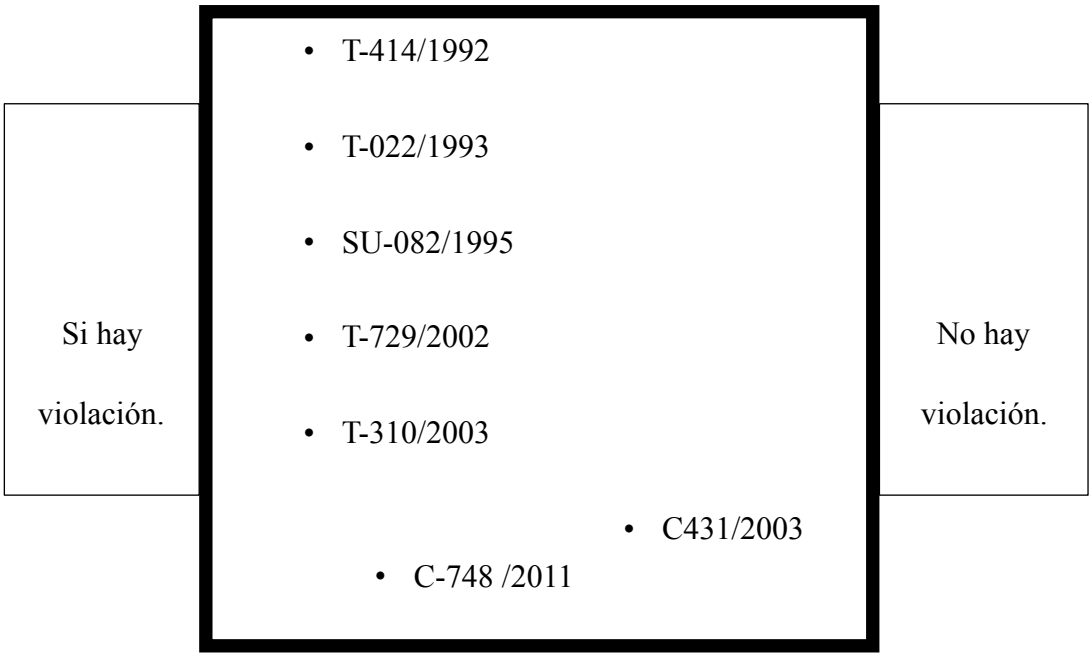
> "Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de:
>
> a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
>
> b) Datos de naturaleza pública.
>
> c) Casos de urgencia médica o sanitaria.
>
> d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

e) Datos relacionados con el Registro Civil de las Personas.” (Colombia, 2012)

Excepciones que son justificadas por la Corte Constitucional en sentencia C-748 de 2011, considerando 2.12.3; especificando que “lo que busca el legislador estatutario es que en los casos taxativos permitidos por el artículo 10, en los que no es necesario el consentimiento del Titular, el uso del dato **también debe sujetarse a todos los principios y limitaciones consagrados en la Ley.** Por el contrario, jamás podría interpretarse como una autorización abierta para que se accedan a datos personales sin consentimiento de su titular.

Gráfico del Análisis Jurisprudencial de sentencias de 1992 - 2015.

¿Hay violación del Derecho a la protección de datos personales (artículo 15. C.P.) Cuando cámaras de vídeo vigilancia recaban datos personales sin autorización del titular?



Fuente: Esquema de línea jurisprudencial, situación fáctica comprendida dentro del limite del escenario constitucional. Elaborado por: Edward Andrés Beltrán López.

Podemos concluir que a los largo de 20 años de ejercicio del Derecho a la Protección de Datos Personales, se ha mantenido en una línea jurisprudencial bien definida, reconociendo que para el tratamiento de datos personales, es indispensable la autorización del titular de los datos, como también que dicha autorización no podrá ser tacita, sino que debe cumplimentar todas las cualificaciones del consentimiento, es decir, libre, previa y expresa.

Las únicas excepciones que se deben tener en cuenta frente a a la autorización son las contenidas en la sentencia C 431 de 2003 y en el artículo 10 de la Ley E. 1581 de 2012.

Dichas excepciones son: (i) Actividades de incursión y seguimiento ejercida por las autoridades judiciales para impedir la ejecución o consumación de conductas punibles, garantizando los requisitos constitucionales y legales, exigiendo que la decisión se motive expresamente para facilitar el control preventivo de las conductas delictuosas y garantizar el derecho a no ser molestado ni individualmente ni en su familia cuando no existan los motivos previstos por la ley para el efecto, además que dichas actividades de incursión o seguimiento pasivo deben ser temporales y realizadas de manera razonable; (ii) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; (iii) Datos de naturaleza pública; (iv) Casos de urgencia médica o sanitaria; (v) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; y (vi) Datos relacionados con el Registro Civil de las Personas."

Análisis estático de la autorización en la Sentencia C 748 de 2011

Con la sentencia C-748 de 2011 se hace control constitucional a la Ley Estatutaria No. 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales" en ella se encuentran definidos los principios, derechos y obligaciones que gobiernan el tratamiento de datos personales, en esta sentencia hito la Corte Constitucional afirma que el artículo 15 de la constitución política reconocen tres derechos fundamentales, siendo estos "(i) el derecho a la intimidad, (ii) el derecho al buen nombre y (iii) el derecho al habeas data." (Colombia, Corte Constitucional 2011)

Si bien, el derecho al habeas data se encuentra en conexidad con los derechos a la intimidad y al buen nombre, todos estos derechos son considerados para la constitución como autónomos y diferentes.

Como punto de partida y con sujeción a la sentencia C-748 de 2011 se señala el alcance material de la Ley Estatutaria 1581 de 2012, que expone:

> "Sin importar la finalidad que tenga la base de datos, mientras esta contenga información y datos personales se deberá respetar los principios generales que regulan el tratamiento y protección de datos; así lo ha sostenido en reiteradas ocasiones la Corte Constitucional al enunciar el desarrollo y alcance que deben tener los principios que regulan el tema de la protección de la información. Una legislación unificada y clara sobre el tema en desarrollo se hace completamente necesaria respondiendo siempre a los principios de necesidad y proporcionalidad, motivo por el cual pretender dejar bases de datos sin que les sea aplicable los principios de la administración de datos, solo debería hacerse en respuesta a un estudio particular de

> cada caso que sobre fundamentos verídicos y con argumentación suficiente que permita, a través del test de razonabilidad, decidir y motivar por qué no se aplicarán los principios básicos que desarrolla un derecho fundamental, basta con analizar desde la óptica de la Corte los principios de libertad, necesidad, veracidad, integridad, finalidad. Y su importancia en el desarrollo del derecho fundamental al Hábeas Data, la protección de datos personales y la autodeterminación informática.". En este caso, la Sala encuentra que el proyecto solamente pretende desarrollar el habeas data y no los otros derechos, por lo que si bien la disposición no desconoce la Carta por ser amplia en este respecto, debe entenderse que solamente desarrolla indirectamente los derechos a la intimidad y al buen nombre, es decir, no puede considerarse una regulación comprensiva y sistemática de tales derechos." (Colombia, Corte Constitucional 2011)

Como se puede observar la Corte fue muy precisa en definir el alcance material de la ley, siendo estrecha en el derecho a la protección de datos personales y amplía en los derechos conexos a este. Con base a dicha interpretación, podemos concluir que cualquier tipo de base de datos –incluyendo los sistemas de videovigilancia- deberán cumplir como mínimo con los principios que gobiernan en su hermenéutica el artículo 15 Constitucional.

Ahora en lo concerniente a la autorización, la Corte señala "que el consentimiento es un aspecto medular del derecho al habeas data y que pese a las múltiples intervenciones que solicitan la inexequibilidad del vocablo "expreso", la definición será declarada ajustada a la Constitución" (Subrayado fuera del texto) (Colombia, Corte Constitucional 2011)

La Corte se hizo aun más extensiva acerca de la autorización, en la interpretación que hace al principio de Finalidad la corte precisó que:

> "los datos personales deben ser procesados con un propósito específico y explícito. En ese sentido, la finalidad no sólo debe ser legítima sino que la referida información se destinará a realizar los fines exclusivos para los cuales fue entregada por el titular. Por ello, se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y por tanto, no podrá recopilarse datos sin la clara especificación acerca de la finalidad de los mismos." (Colombia, Corte Constitucional 2011) (Subrayado fuera del texto.)

Por su parte, con el principio de Libertad se precisa que solo puede aplicar tratamiento a datos personales bajo el consentimiento previo, expreso e informado del titular de los mismos y que todo dato obtenido o divulgado sin la previa, expresa e informada autorización por parte del titular o en ausencia de orden judicial o mandato legal, será considerado ilegal y lesiona el derecho al habeas data.

Conforme a la sentencia C-748 de 2011 "El principio de libertad, pilar fundamental de la administración de datos, permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos. También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente." (Colombia, Corte Constitucional 2011) (Subrayado fuera del texto)

Como podemos observar, la autorización esta intrínsecamente ligada con el principio de libertad, y sin ella como lo reitera la Corte en sentencia C-748 de 2011:

> "la posibilidad de acumular informaciones en cantidad ilimitada, de confrontarlas y agregarlas entre sí, de hacerle un seguimiento en una memoria indefectible, de

objetivizarlas [sic] y transmitirlas como mercancía en forma de cintas, rollos o discos magnéticos, por ejemplo, permite un nuevo poder de dominio social sobre el individuo, el denominado poder informático." (Colombia, Corte Constitucional 2011)

Resumiendo, para que exista una vulneración del derecho a la protección de datos personales,

> "debe desconocerse alguno de los tres aspectos enunciados. Es decir, la información contenida en el archivo debe haber sido recogida de manera ilegal, sin el consentimiento del titular del dato (i), ser errónea (ii) o recaer sobre aspectos íntimos de la vida de su titular no susceptibles de ser conocidos públicamente (iii). Por el contrario, el suministro de datos veraces, cuya circulación haya sido previamente autorizada por su titular, no resulta, en principio, lesiva de un derecho fundamental." (Colombia, Corte Constitucional 2011)

Ahora en lo referente a los datos sensibles la Corte sostiene que la prohibición no solo es sostenible con la Constitución Política, sino que se hace exigible por derechos conexos como la intimidad y la dignidad humana, un desarrollo al principio de habeas data de acceso y circulación restringida, además sostuvo que:

"Ciertamente, como se explicó en la sentencia C-1011 de 2008, en tanto los datos sensibles pertenecen a la esfera de la intimidad de las personas, "(…) todo acto de divulgación mediante los procesos genéricos de administración de datos personales, distintos a las posibilidades de divulgación excepcional descritas en el fundamento jurídico 2.5. del presente análisis, se encuentra proscrita. Ello en la medida que permitir que información de esta naturaleza pueda ser objeto de procesos ordinarios de acopio, recolección y circulación vulneraría el contenido esencial del derecho a la intimidad." (Colombia, Corte Constitucional 2011)

Además en su considerando 2.8.4.1 de la sentencia, la corte aplico la técnica de modulación integradora señalando que si el dato sensible es tratado sin autorización del titular, bien sea porque es requerido por una ley o por las limitantes expuestas aquí, "siempre y cuando se entienda, como se mencionará más adelante, que tal autorización, además de estar contenida en una ley, sea conforme a las garantías que otorga el habeas data, por ejemplo en materia de finalidad, y cumpla las exigencias del principio de proporcionalidad." (Colombia, Corte Constitucional 2011)

Sin embargo, existe una excepción que se puede plantear en el supuesto fáctico de sistema de vídeo vigilancia implementado por el estado y es que:

> "tanto en el ordenamiento internacional como en el derecho comparado, se disponen causales que eximen la necesidad de la autorización. Así, en la Resolución 45/95 del 14 de diciembre de 1990 de las Naciones Unidas, se consagran restricciones relacionadas con la "seguridad nacional, orden público, salud pública o la moralidad; así como para proteger los derechos y libertades de otros, especialmente las personas que estén siendo perseguidas, siempre que tales excepciones estén especificadas de forma explícita en una ley o norma equivalente, promulgada de acuerdo con el sistema jurídico interno, que expresamente establezca sus límites y prevea las salvaguardas adecuadas" (Colombia, Corte Constitucional 2011)
>
> Como resultado del análisis estático, y en consonancia a el análisis dinámico y estático del precede de la Corte Constitucional y las disposiciones de la Ley Estaturia No. 1581 de 2.012, resulta de nuevo la afirmación de que la autorización o la autodeterminación informática es considerada como el "pilar fundamental del habeas data," la cual debe ser libre, previa y expresa o exceptuada mediante un

expreso mandato legal o mediante una orden de una autoridad judicial y sin ella se lesiona en directo el Derecho Fundamental a la Protección de Datos Personales.

La autorización y sus principios

En cuanto a la autorización, logramos identificar que la misma es considerada por la Corte Constitucional, como el aspecto medular que da origen al tratamiento de datos personales, además de facultar al titular de los datos en poder autodeterminar su información informática. Que para el caso en relación es la concerniente a los datos de imagen que captan las cámaras de vídeo vigilancia en Colombia.

No obstante, el paso a seguir es identificar que se entiende por autorización y cuales son las formas de obtenerla en el tratamiento de datos sensibles.

Dicho lo anterior, la autorización en la Ley E. 1.581 de 2012 en su artículo 3º es entendido como *"el consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales."* (Colombia, 2012)

Con base en (Colombia, Superintendencia de Industria y comercio 2012), y lo señalado anteriormente por la jurisprudencia; se entenderá por previo, que la autorización debe ser suministrada en una etapa anterior a la del dato; se entenderá por expreso, que la autorización debe ser inequívoca, razón por la cuál no se permite un consentimiento tácito; se entenderá por informado, cuando se le informe de manera clara al titular las disposiciones que gobiernan el tratamiento de datos, como por ejemplo, la finalidad, el uso, la necesidad, entre otros.

Por su parte, el decreto 1377 de 2013 *"que reglamenta parcialmente la Ley E. 1581 de 2012."* en su artículo 5º señalo que:

> *"El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así*

como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento." (Colombia, 2013)

Entonces, es momento de identificar las formas contempladas en el artículo 7º del Decreto 1377 de 2013 de obtención de la autorización, las cuales son:

I. Por escrito

II. De forma oral

III. Mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.

Una manera de poder ejemplificar la primera situación es cuando el titular acepta **por escrito**, es decir, cuando en un documento el titular estampa allí su firma. En la segunda situación fáctica, **de forma oral**, aplica cuando por medio de las grabaciones el titular otorga autorización. Sin embargo recordemos que la norma es clara y señala en el Artículo 8° del Decreto 1377 de 2013 que se deberá tener "***Prueba de la autorización.*** Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos." (Colombia, 2013)

De la autorización para el tratamiento de datos sensibles.

Por ahora solo basta con señalar la normatividad que regula el tema, comenzando desde los procedimental a lo sustancial. Empezare por señalar lo contenido en el Decreto 1377 de 2013.

*"**Artículo 6°. De la autorización para el Tratamiento de datos personales sensibles**. El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley. En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6° de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:*

1. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.

2. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.

Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles." (Colombia, 2013)

En consonancia con lo propuesto por Alexy (2014) la norma que se sustrae de dicho enunciando resalta que: Se encuentra prohibido el tratamiento de datos sensibles a excepción de lo contemplado en el artículo 6º de la Ley Estatutaria No. 1581 de 2012 -que veremos a continuación- y que deberán cumplirse 2 obligaciones; (i) informar la no obligación de autorizar su tratamiento y (ii) obtener su consentimiento expreso.

" Artículo 6° en mención, el cual señala: ***Tratamiento de datos sensibles.*** Se prohíbe el Tratamiento de datos sensibles, excepto cuando: a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización; b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización; c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos

> no se podrán suministrar a terceros sin la autorización del Titular; d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares." (Colombia, 2012)

Así que, como se puede inferir de la extracción de la norma y parafraseando en referencia a (Colombia, Superintendencia de Industria y Comercio 2013), en su pagina 17 y siguientes: la vídeo vigilancia resulta aplicable a la Ley E 1581 de 2012, se deben observar y respetar los principios contenidos en la normar. Dicho lo anterior y en referencia a los datos biométricos, señalo que en el caso particular no dicha hipótesis no se enmarca dentro de los literales b,c,d y e por lo cual se debe enmarcar en el literal a. Siempre y cuando no se entienda que para el tratamiento de datos sensibles es valida la autorización a través de conductas inequívocas.

Principios en la protección de datos personales.

Retomando la teoría propuesta por Alexy (2014), se examinara el significado de principio y su optimización en los derechos fundamentales.

Dentro de la teoría ha existido una discusión en referencia a reglas y principios. La reglas son entendidas como las expresiones deónticas básicas como el mandato, el permiso y la prohibición, por ejemplo: Se prohibe el tratamiento de datos sensinbles. Mientras que los Principios, son entendidos como las razones de llevar a cabo juicios del deber ser.

Los principios parafraseando a Alexy (2014, p.80) ordenan que algo debe ser realizado en la mayor medida posible, teniendo en cuenta las posibilidades jurídicas y fácticas. Son mandatos conocidos en una primera instancia como *prima facie.*

Sin embargo, mediante un enfoque más estricto y siguiendo todavía a Alexy (2014, p. 68) podemos inferir que los principios son mandatos de optimización que *"se caracterizan por que pueden cumplirse en diferente grado y que la medida debida de su cumplimiento no sólo depende de las posibilidades reales sino también de las jurídicas."* Ejemplificar esto seria como decir que los principios que gobiernan el Derecho a la Protección de Datos Personales, deberán cumplirse en la medida mayor posible, tanto en los hechos como en la normatividad.

Aún con lo anterior, Alexy (2014, p. 96) señala que *se "tiene validez en la medida en que, no se contrapongan con ningún interés de un rango mayor a los intereses de libertad que la norma protege"*

Entrar a debatir cuales son los principios contrapuestos en relación al presente trabajo, seria extender el campo de acción, incluso sería necesario hacer un estudio en concreto de cuales son los intereses por parte del Estado y de los particulares que gobiernan la vídeo vigilancia, para luego, proceder a realizar la ponderación de principios que señala Alexy en su teoría. Sin embargo, se reitera que el objetivo que se busca es identificar la importancia que tiene la autorización -conocida jurisprudencialmente como la autodeterminación informática- como aspecto medular para el tratamiento de datos sensibles por las cámaras de vídeo vigilancia en Colombia, por tal razón, y siguiendo lo establecido por la Corte Constitucional al referirse a principios señalo que estos se deben entender en la terminología de Robert Alexy y considero:

> *"Estos se tratan de un mandato de optimización que ordena que se realice algo en la mayor medida de lo posible de acuerdo con las posibilidades jurídicas y fácticas, pero cuando colisiona con otros principios como el de salvaguarda de los sistemas de protección social o la sostenibilidad financiera, dicho conflicto tiene que ser ponderado en el caso concreto para determinar si se justifica o no de manera razonable la limitación"* (Colombia, Corte Constitucional 2011)

Desde el año 1992 la corte ha venido desarrollando una serie de principios que deberán gobernar el tratamiento de datos personales: libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad. Además, la Ley Estatutaria. No. 1581 de 2012, en su artículo 2º parágrafo establece que:

> *"Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley."* (Colombia, 2012)

Podemos inferir que los principios que continuación se describirán buscan el deber de la norma fundamental en referencia a la autorización.

Principio de Libertad.

El principio de Libertad, se encuentra enunciado en el artículo 4º literal c de la Ley Estatutaria No. 1581 de 2012:

"El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento." (Colombia, 2012)

La Corte en la sentencia C-748 de 2011, argumento que:

"**los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo y expreso del titular**. La Corporación ha relacionado el principio de libertad, con la prohibición del manejo de la información adquirida de manera ilícita, de tal forma que se encuentra prohibida la obtención y divulgación de los mismos, sin la previa autorización del titular o en ausencia de mandato legal o judicial. Así, en la sentencia SU-082 de 1995, afirmó: "*los datos conseguidos, por ejemplo, por medios ilícitos no pueden hacer parte de los bancos de datos y tampoco pueden circular."* En el mismo sentido, en la Sentencia T-176 de 1995, se consideró como una de las hipótesis de la vulneración del derecho al habeas data el de la recolección de la información "*de manera ilegal, sin el consentimiento del titular de dato*."(Colombia, Corte Constitucional 2011)

De esta forma es como nuevamente se reitera que para poder realizar el acopio de los datos personales recogidos por la cámaras de vigilancia, es necesario que el propietario solicite la autorización al titular del dato, de lo contrario estaríamos en frente de la vulneración al derecho fundamental.

Además como lo señalo la Corte, los principios deben ser entendidos como mandatos de optimización, los cuales deberán cumplirse en la medida mayor posible para garantizar el derecho fundamental.

Principio Finalidad.

Contemplada en el artículo 4º literal b de la Ley Estatutaria No. 1581 de 2012, establece que "El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular." (Colombia, 2012)

Pues como se observa no lleva enunciado el vocablo autorización, es muy importante para el mismo, ya que, cuando el titular del dato conoce la finalidad con la que van a ser tratados sus datos personales, puede dar una autorización libre, expresa e informada. Además que, una vez cumplida la finalidad en el tratamiento el responsable o encargado deberá proceder a la eliminación o retiro del dato de su base de datos.

Señala la corte como derivación del derecho a la autodeterminación informativa, la facultad de poder exigir "el adecuado manejo de la información que el individuo decide exhibir a los otros"(Colombia, Corte Constitucional 2011). Por lo tanto, según este principio "tanto el acopio, el procesamiento y la divulgación de los datos personales, debe obedecer a una finalidad constitucionalmente legítima, definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos, así como el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista."(Colombia, Corte Constitucional 2011)

Principio de necesidad.

Este principio establece que los datos personales registrados deben ser los estrictamente necesarios para el cumplir con las finalidades perseguidas en la recolección de datos, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos.

Por su parte la Corte Constitucional señalo que "la información solicitada por responsable, debe ser la estrictamente necesaria y útil, para alcanzar la finalidad constitucional perseguida. Por ello, los datos sólo pueden permanecer consignados en el archivo mientras se alcanzan los objetivos perseguidos. Una vez esto ocurra, deben desaparecer." (Colombia, Corte Constitucional 2011)

Datos sensibles

Con un bosquejo como el anterior y considerando avanzar frente al tema que nos ocupa; cada vez que una cámara de vídeo vigilancia realiza su accionar, es decir, recaba datos personales de clasificación sensible, veamos que se entiende por dato sensible:

> Artículo 5º. Datos sensibles: Son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelan el origen étnico. La orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos (Colombia, 2012)

En efecto, la Corte en la sentencia C-1011 de 2008, señalo que:

"la información sensible es aquella *"(...) relacionada, entre otros aspectos, con la orientación sexual, los hábitos del individuo y el credo religioso y político.* ***En estos eventos, la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad, entendido como aquella 'esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerado un elemento esencial del ser,*** *se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico.* (Negrillas fuera del texto.) (Colombia, Corte Constitucional 2008)

Teniendo claro el concepto de dato sensible, concluyendo que este puede afectar en mayor medida la vida y dignidad de una persona, además que tiene la facultad de

identificarla mejor, es necesario pasar a conocer que se entiende por dato bihométrico y cuales son las formas de reconocimiento que se aplican.

Datos Biométricos

La palabra biometría se deriva de sus raíces griegas bio=vida y metría=medición o medida, y se define como un "Estudio mensurativo o estadístico de los fenómenos o procesos biológicos" (RAE, 2015). Con base al International Group, el cual señala que, "biometrics es el uso automatizado de las características físicas y de comportamiento de una persona para determinar o verificar su identidad." (Remolina y Gómez, 2014, p. 225).

Conforme los establece (Remolina y Gómez, 2014) los sistemas de identificación biométrica identifican y verifican a un individuo respecto a sus características biológicas, morfológicas, anatómicas y rasgos de comportamientos de personas, estos datos son irrepetibles e intransferibles. Estos sistemas se clasifican en dos sistema de medición: Los primeros se basan en la medición de las características (Biométria Estática) y los segundos se basan en la medición de comportamientos (Biométria Dinámica) (Remolina y Gómez, 2011, p. 224), como lo veremos a continuación en el siguiente cuadro, que nos define y explica algunos ejemplos, veamos:

Cuadro 1. Sistemas de identificación y verificación biométrica basados en características físicas y de comportamiento de cada persona.

	Método	Descripción
FÍSICAS	Reconocimiento facial	Utilizan una cámara para tomar una foto del rostro de la persona. De la imagen se extraen elementos particulares (características relacionadas con las facciones) que luego se comparan con un banco de datos de imágenes en la que previamente esta la foto de la persona que se busca identificar.
	Termografía Facial	Usan las diferentes temperaturas que emanan de las partes del rostro de un individuo, como elementos específicos para caracterizar e identificar a una persona.
	Reconocimiento de Huellas Dactilares	Emplea los patrones particulares de las huellas dactilares que distinguen una persona de otra.
	Geometría de la Mano	Utilizan la medida, dimensión y forma particular de la mano de cada persona.
	Escaneo del Iris	Compara la imagen del iris de una persona tomada, con una cámara frente a las que previamente se encuentran en una base de datos. Se analizan los patrones característicos de este tejido que circunda la pupila.
	Escaneo de la Retina	Utiliza rayos láser para escanear los parámetros distintivos de los vasos sanguíneos de la retina de una persona y los compara con patrones previamente almacenados de la misma.
	Reconocimiento de los Vasos Sanguíneos de las Manos	Usan luces infrarrojas para determinar el patrón del comportamiento de las venas de las mano.

	Método	Descripción
	Huellas Labiales	Los labios tienen patrones característicos (Huellas Labiales) y formas particulares que permiten identificar a una persona.
	Reconocimiento de los Huesos	Los huesos de cada de individuo pueden ofrecer particularidades que permitan su identificación confiando con aspectos como la densidad ósea o cicatrices de lesiones anteriores.
	Método	**Descripción**
COMPORTAMIENTO	Reconocimiento del Patrón de Marcha	Utiliza como característica de identificación la forma particular de caminar de cada individuo.
	Patrón del Movimiento del Mouse	Se funda en las característica del comportamiento (velocidad, precisión) del individuo en el uso del mouse.
	Análisis de la Firma	Utiliza los patrones estáticos (que pueden ser imitados por un experto) y dinámicos (como la presión, la dirección y la velocidad, que son de difícil simulación) de una persona cuando firma.
	Verificación de la Voz	El reconocimiento de la voz se funda en datos físicos (características de la vía aérea) y dinámicos (movimientos de la boca y pronunciación). La voz de la persona se compara con su "patrón de voz" previamente almacenado.
	Patrones de Tipeo	Cada individuo tiene un patrón y cadencia particular de tipeo en el teclado, evaluándose los tiempos de latencia y de presión en cada tecla.

Nota: Tomado de: (Remolina y Gómez, 2011, p. 228) El cuadro es una versión adaptada y ampliada de la publicada en FURNELL, STEVEN Y NATHAN, "Biometrics: no silver bullets", op.cit., pág.9.

Ahora, frente a los sistemas de videovigilancia situación fáctica que nos interesa podemos observar que ambos sistemas de biométria son aplicables, pues, la biométria estática se aplica con el reconocimiento facial, la termografía facial y el escaneo del iris, mientras que la biometria dinámica ese aplica con el reconocimiento del pratón de marcha y la verificación de voz que nos enseña y describe el cuadro No. 1.

Más adelante cuando hablemos de las características de las cámaras señalare las nuevas funcionalidades de las cámaras frente a estas nuevas formas de análisis de datos biométricos hasta aquí aprendidas, por ahora se continuara con el desarrollo del trabajo.

Cuando hablamos de mecanismos biométricos nos estamos refiriendo al tratamiento de información sensible, podemos llamar datos biométricos a los siguientes: El ADN, el rostro, la huella dactilar, geometría de la mano, venas de la mano, el iris, el escaneo de retina, la voz, la firma, el olor, el modo de caminar, el oído, la contextura, el comportamiento, la imagen física de una persona en movimiento.

Para el tratamiento de estos datos sensibles, como los señala (Remolina y Gómez, 2011) existen dos sistemas de autenticación el primer sistema de autenticación humana por sus siglas en inglés (Human Authentication System) que compara entre muchas variables, el cabello y la voz de una persona, con la información que tiene sobre ella previamente en una base de datos, el resultado depende del juicio de valor de una persona, y los sistemas biométricos de autenticación, por sus siglas en inglés (Biometric Authentication System) aquí el reconocimiento es inmediato sin necesidad de una persona que realice la comparación.

Para poder de la autenticación debemos primero conocer algunas variables de la misma y que nos permitirán entender el cuadro 2. De acuerdo con (Remolina y Gómez, 2011, p. 239):

- Unicidad: En el entendido que solo esa persona tiene ese patrón biométrico.
- Permanencia: Denota qué tan invariable es la característica biometrico con el paso de tiempo.
- Precisión: Establece qué tan exacto o infalible es el sistema biométrico para establecer la absoluta identidad de una persona.
- Aceptabilidad: Se refiere a qué tanto las personas están dispuestas a aceptar determinado sistema biométrico.
- Seguridad: Establece qué tan fácil es manipular los sistemas biométricos mediante técnica fraudulenta.

Cuadro 2. Comparación de sistemas biométricos.

Sistema Biométrico	Unicidad	Permanencia	Precisión	Aceptabilidad	Seguridad
ADN	Alto	Alto	Alto	Bajo	Bajo
Rostro	Bajo	Medio	Bajo	Alto	Bajo
Huella Dactilar	Alto	Alto	Alto	Medio	Alto
Geometría de la Mano	Medio	Alto	Medio	Medio	Medio
Patón del teclado	Bajo	Bajo	Bajo	Medio	Medio
Venas de la mano	Medio	Medio	Medio	Medio	Alto
Iris	Alto	Alto	Alto	Bajo	Alto
Escaneo de retina	Alto	Medio	Alto	Bajo	Alto
Firma	Bajo	Bajo	Bajo	Alto	Bajo
Voz	Bajo	Bajo	Bajo	Alto	Bajo
Olor	Alto	Alto	Bajo	Medio	Bajo
Modo de andar	Bajo	Bajo	Bajo	Alto	Medio
Odio	Alto	Medio	Medio	Alto	Medio

Nota: Tomado de: (Remolina y Gómez, 2011, p. 239) La información contenida en esta tabla se tomó de Jain Anil (Ed.), *Biometrics: personal Identification in networked society, op, cit., pág. 16.*

Como podemos notar en el cuadro, en el supuesto fáctico que nos interesa, las cámaras de seguridad cuando captan el rostro y la forma de caminar presentan debilidades frente a la precisión y seguridad del dato, a menos que se utilicen programas de reconocimiento facial, pues ellos si permiten comparar por lo menos el rostro del individuo para hacer la autenticación.

Reconocimiento facial, de orejas y termograma del rostro.

Con base a (Remolina y Gómez, 2011, p. 235) señala que:

> El reconocimiento facial se basa en el análisis de ciertos puntos clave en en rostro de las personas, como la distancia de los ojos, el diámetro nasal, las orejas o la boca. El aumento masivo de uso de cámaras de videos en lugares públicos y privados ha puesto de presente la relevancia del reconocimiento facial como medio de autenticación e identificación. Al mismo tiempo, esta situación ha generado preocupación en la doctrina por le grado de vigilancia de las personas, que en algunos casos llega a ser considerado excesivo e intrusivo.

Parafraseando a (Remolina y Gómez, 2011), los sistemas de videovigilancia tiene la ventaja que no necesitan del contacto con el titular para poder obtener sus datos personales, pero que se enfrentan a desventajas como son: la falta de iluminación, la distancia, el clima, el vejez de la cámara, las alteraciones faciales, etc., y que a su vez se debe resaltar que estos sistema biométricos permiten registrar de manera paralela elementos relacionados con el estado emocional de las personas y que cuando ademas de la grabación de la imagen se capta

la voz de la persona podemos lograr no solo la afectación del derecho a la protección de datos sino que nos encontraríamos en conexidad con otros derechos como la privacidad, intimidad y el más importante la dignidad humana.

Sujetos intervinieres en los sistemas de vídeo vigilancia

Como se expuso anteriormente, en la sentencia hito SU-082 de 1995 se precisaron los sujetos que intervienen en el derecho a la protección de datos personales, considerando que el sujeto activo "es toda persona, física o jurídica, cuyos datos personales sean suceptibles (Sic) de tratamiento automatizado."(Colombia, Corte Constitucional 1995) y por sujeto pasivo definió "toda persona física o jurídica que utilice sistemas informáticos para la conservación, uso y circulación de datos personales." (Colombia, Corte Constitucional 1995)

En referencia a los conceptos anteriormente descritos, toda persona que sea grabada utilizando los sistemas de videovigilancia será considerada para efectos de este artículo sujeto activo y por ende, toda persona natural o jurídica, entidad pública o privada que utilice sistemas de video vigilancia será considerada para efectos de este artículo sujeto pasivo.

Sujetos pasivos

De acuerdo a la ley, pueden existir varios sujetos pasivos, en primer lugar encontramos en la Ley E. No. 1581 de 2012 artículo 3º, literal (e) al Responsable del Tratamiento: "Persona natural o jurídica , pública o privada, que por si misma o en asocio con otros, decida sobre la base de datos y/o tratamiento de datos." (Colombia, 2012) Parafraseando a Remolina (2013, p. 114) Podría decirse que el responsable es el dueño de la base de datos o archivo, se trata del sujeto que directa o indirectamente recolecta los datos y define los usos junto con las demás actividades que desprenden del tratamiento del mismo,

que para el caso de las cámaras de videovigilancia serian los propietarios o dueños de las mismas.

Luego en el literal (d) de la misma Ley encontramos al Encargado del tratamiento: "Persona natural o jurídica , pública o privada, que por si misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable de tratamiento." (Colombia, 2012). Parafraseando a Remolina (2013, p. 116) el encargado obra en nombre del responsable de tratamiento, realiza cualquier actividad u operación que se le ordene, por ello si el encargado ha de efectuar una mala practica en el tratamiento que le realice a los datos deberán entonces responder solidariamente entre el responsable y el encargado.

Para poner un ejemplo, cuando el propietario de las cámaras compra una dirección Ip y sube la captación de las cámaras a la nube, como lo veremos más adelante, si el operador o proveedor que contrato realiza una mala práctica como en el caso de insecam[7] respondería solidariamente por los daños y perjuicios que se ocasiones debidos a la mala practica.

Finalmente los usuarios, pueden ser las personas naturales o jurídicas, que por si mismas o en asocio con otros, usen y/o utilicen los datos personales a que tienen acceso, personas que fueron excluidas de la Ley Estatutaria No. 1581 de 2012, pero que conforme lo señala Remolina (2013, p. 122.) la corte luego los consideró que en ocasiones pueden ser los mismos responsables y ademas señalo en que:

> "Todos los principios de las administración de datos personales […] son oponibles a todos los sujetos involucrados en el tratamiento del dato, entiéndase en la recolección, circulación, uso, almacenamiento, supresión, etc., sin importar la

[7] Disponible en: http://www.insecam.org Sitio Web que permite la visualización en línea de 94 cámaras de seguridad en Colombia. Fecha de consulta marzo 1 de 2016.

> denominación que los sujetos adquieran, es decir, llámense fuente, responsable del tratamiento, operador, encargado del tratamiento o usuario, entre otros" (Colombia, Corte Constitucional 2011)

Sujeto activo

El sujeto activo, conforme a la (Colombia, 2012) es definido como la "persona natural cuyos datos personales sean objeto de Tratamiento", es decir, las personas que son grabadas, filmadas, monitoreadas por las cámaras de videovigilancia.

Como lo define Remolina (2013, p. 113) se trata del sujeto jurídico protegido por la Ley E. No 1581 de 2012, razón por la cual la misma le confiere unos derechos y exige a los responsables y encargados que respeten ciertos mínimos legales cuando traten su información.

El titular del dato, es la persona más importante en todo el tratamiento y acopio de datos, pues es la única propietaria, dueña, poseedora de su información personal, y no como se señala, que el dueño de la base de datos es el dueño de la información. Concepto que será muy difícil de erradicar mientras no se tome más conciencia a la hora de entregar nuestra información personal.

Los sistemas de vídeo vigilancia

En la actualidad, los sistemas de videovigilancia son una practica muy extendida en nuestra sociedad. Dichos sistemas son utilizados con el supuesto de hecho de garantizar una seguridad pública y privada en un país con tantos conflictos e inseguridad como Colombia.

La Agencia Española de Protección de Datos (AEPD) en su guía sobre la videovigilancia , describe que generalmente esta "persigue garantizar la seguridad de los bienes y las personas o se utiliza en entornos empresariales con la finalidad de verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales. Ambas finalidades constituyen bienes valiosos dignos de protección jurídica, pero sometidos al cumplimiento de ciertas condiciones. La utilización de medios técnicos para la vigilancia repercute sobre los derechos de las personas lo que obliga a fijar garantías." (España, Agencia Española de Protección de Datos 2014)

Las cámaras de vídeo vigilancia.

Primero definamos que se entiende por cámara: Una cámara es un aparato o maquina que a través de una lente permite registrar imágenes estáticas o en movimiento. (Larousse, 2003). Ahora pasemos a recordar la evolución que ha tenido la cámara desde análogas a digitales:

Cámaras análogas: Aparecen a principios de 1960 y eran llamadas VTR por sus siglas en ingles (Video Tape Recorder) Grabadora de Cinta de Video. Estas cámaras son capaces de capturar imágenes y guardarlas en soporte magnéticos. Lopez. R (2007, p.7.)

Camara digital: Se define como un dispositivo electrónico usado para capturar y almacenar fotografías electrónicamente en lugar de usar películas fotográficas como las cámaras análogas. La cámara digital se compone de pixeles y los convierte en un numero. Lopez. R (2007, p. 9)

Teniendo claro estos conceptos pasemos a clasificar en solo dos las cámaras que nos interesan: Cámaras de video digital con circuitos cerrados de T.V. y las cámaras IP.

Las cámaras digitales son aquellas cuyo principal uso es captar imágenes en un formato Digital, parafraseando a Lopez. R. (2007, p. 17) Usan una memoria interna para el almacenamiento de imágenes o para realizar la transferencia, aunque son muy pequeñas pueden conectarse con otros dispositivos los cuales permitir el almacenamiento en gran medida.

Los circuitos cerrados de T.V. son sistemas de videovigilancia que operan conectando todo el sistema de cámaras a unos monitores los cuales permiten visualizar las imágenes recabadas por la cámaras de seguridad. Los circuitos de T.V. pueden operar con la sola transmisión de las imágenes en tiempo real o se pueden instalar grabadores de video en red.

> Las cámaras IP (Internet Protocolo) o cámaras en red son cámaras de video digital combinadas con una computadora en una unidad inteligente; capturan y transmiten imágenes digitales en vivo directamente a través de cualquier red IP,

> permitiendo a los usuarios ver y/o manejar la compra de forma remota a través de un servidor Web, en cualquier lugar y en cualquier momento. Lopez. R. (2007, p. 20)

Conectividad IP

Con base a la definición sugerida de cámara IP, pasare a explicar lo referente a la su arquitectura y funcionamiento. La conectividad IP para sistemas de videovigilancia sin duda son las más utilizadas en la actualidad, pues como es conocido, desde los hogares, locales comerciales, bancos, entidades estatales, tienen estas cámaras para vigilar sus intereses.

Como funciona la conectividad IP, primero debemos saber que es una dirección IP:

> La IP es necesaria para conectarse a la red. Se reconoce mediante una serie de números expresados en bytes que son asignados a los computadores de quienes quieren ingresar a la red y sin los que es imposible navegar en ella. Un PPP asigna los IP, que son de vital importancia para circular por la red, debido a que el protocolo utilizado en la Internet (TCP/IP), es el que hace posible la comunicación entre todos los usuarios que ingresan a la red con un IP. Además de los protocolos IP y TPC/IP, también es necesario para navegar el protocolo UDP o protocolo de data grama del usuario; que permite el envío de un mensaje desde un computador a una aplicación que se ejecuta en otro equipo. (Álvarez y Garzón, 2009)

Entonces, las cámaras IP tienen sus propias direcciones IP, las cuales le permiten conectarse directamente con la red como cualquier dispositivo -vgr. celular- estas cámaras

además cuentan con un software llamado, Protocolo de transferencia de archivos, que permite como su nombre lo indica transferir archivos, los cuales pueden ser vistos a través de una cuenta y contraseña que el cliente tiene para conectarse a la red.

Al contar ya con sistemas digitales de videovigilancia, los sistemas análogos fueron desapareciendo ya que son menos eficientes al actual. Con la ayuda del internet de las cosas, las cámaras empezaron a tener su propia IP como se explico anteriormente, permitiendo agilizar la conectividad para el fin buscado. Parafraseando a Lopez. R. (2007, p. 83) con un sistema digital, se pueden conectar tantas cámaras como le sea posible.

Sistemas de almacenamiento en los sistemas de vídeo vigilancia.

Para poder llevar a cabo los sistemas de videovigilancia, debemos hablar sobre los sistemas de almacenamiento, veamos: Existen 2 tipos de almacenamiento que sirven para el sistema de videovigilancia, el primero de ellos, es el llamado almacenamiento directamente conectado y el almacenamiento desconectado.

El almacenamiento directamente conectado es la información que es almacenada en un disco local C, los discos duros pueden estar ubicados en las computadoras encargadas de ejecutar la función, como también pueden estar integrados dentro de dispositivos de almacenamiento llamados DVR (Grabador de Video Digital).

En el segundo, la información puede ser almacenada contratando un servicio de Cloud. Los servicios Cloud son entendidos como:

La computación en nube es un modelo para permitir , conveniente, acceso ubicuo a la red bajo demanda a una compartida conjunto de recursos informáticos configurables (por ejemplo , redes , servidores, almacenamiento , aplicaciones y servicios) que puede ser aprovisionado y puesto en libertad con mínimo esfuerzo de administración o la interacción proveedor de servicios rápidamente. Este modelo de nube se compone de cinco características esenciales, tres modelos de servicio, y cuatro de despliegue modelos. (Instituto Nacional de Estándares y tecnología , 2011)

En el primer modelo de almacenamiento -Disco local C- siempre y cuando la unidad de Disco se encuentre en Colombia, es decir, dentro de las instalaciones de una empresa, entidad estatal o vivienda, le será aplicable la legislación colombiana, y por ende la Ley Estatutaria 1581 de 2012.

Mientras que, en el modelo segundo, los servicios de almacenamiento Cloud, dichos data centers se encuentran ubicados en el exterior, por lo tanto la información viaja de Colombia a diferentes países y dependiendo de la ubicación de los datos, les será aplicable la legislación del país donde se encuentra ubicado el data center. Es decir, que las empresas, entidades y particulares que contraten servicios de Cloud, deberán haber solicitado la autorización del titular del dato para poder realizar la transferencia internacional de los datos y transferir los datos a terceros. A su vez, deberán contractualmente acordar cláusulas para la satisfacción de dichas medidas.

Los servicios de Cloud, por lo general cumplen con las siguientes características: (i) los servicios Cloud computing son contratados mediante contratos de adhesión, donde la parte dominante tiene condiciones de superioridad, estabilidad y salvamento frente al aceptante, (ii) los servicios de almacenamiento se encuentran localizados fuera de Colombia,

es decir, los data center se encuentran localizados en países extranjeros, (iii) al ubicarse los data center fuera de Colombia y al encontrarse los datos almacenados en ellos, gobiernan las leyes del país receptor, (iv) los titulares de los datos, pierden el control total de su información, ya que, esta se encuentra almacenada y duplicada en distintos data center del Prestador de Servicios de Internet, por sus siglas en inglés (ISP) y (v) cuando enviamos las imágenes a la Cloud computing, nos encontramos realizando una transferencia internacional de datos.

Tras haber hecho un recuento de las dos modalidades anteriormente enunciadas, podemos concluir con base en la Ley Estatutaria 1581 de 2012, que para contratar a un proveedor de servicios cloud debemos realizar contratos de transmisión o de transferencia de datos, obligaciones que están a cargo del responsable de la base de datos y se contemplan estipulados en la Ley 1581 de 2012 y el decreto 1377 de 2013 artículo 24 y 25.

Que de acuerdo a la Ley E. No. 1581 de 2012, artículo 26º:

> Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.Esta prohibición no regirá cuando se trate de: a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia; b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública; c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable; d)

> Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular; f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Así las cosas, si se utilizan sistemas cloud para el almacenamiento de las imágenes de los sistemas de videovigilancia, el responsable deberá solicitar la autorización del titular y/o enmarcase dentro de una de las excepciones propuestas.

Conclusión

De manera que, los sistemas de vídeo vigilancia al captar **-tratamiento-** la imagen de una persona, puede identificarla a ella y solo ella **-dato personal-** y dicha información se puede almacenar en una **base de datos.** Por consiguiente que el Derecho a la Protección de Datos Personales es vinculante con los sistemas de vídeo vigilancia dado que se cumple los 2 supuestos principales: Dato y Tratamiento.

En referencia a los Datos Sensibles, como las imágenes que son recolectadas por las cámaras de seguridad, aquellas son entendidas como datos biométricos los cuales pueden dividirse en dos grupos, (i) los físicos y (ii) los de comportamiento, los cuales son recolectados por los sistemas de vídeo vigilancia y se identifican como (i) el rostro, la imagen, la contextura, el color, y (ii) la manera de caminar o comportarse.

Además, gracias al decreto 1377 de 2013 y los diferentes pronunciamientos de la Superintendencia de Industria y Comercio, se pudo inferir que la vídeo vigilancia resulta aplicable a la Ley E 1581 de 2012, y que en ella se deben observar y respetar los principios contenidos en la norma.

Dicho lo anterior, y en referencia al fundamento de norma, se puede concluir que el Derecho a la protección de datos personales, es considerado como Derecho fundamental ya que inicialmente cumple con el carácter precisión, es decir, se encuentre tipificado dentro de los artículo 11 al 41 de nuestra Constitución Política y luego gracias al desarrollo jurisprudencial se ha podido establecer por medio del precedente que este se encuentra adscrito al artículo 15 y tiene completa autonomía frente a derechos conexos como la privacidad, intimidad, honra, entre otros.

En consecuencia, el Derecho Fundamental a la Protección de Datos Personales, puede ser considerado como aquel derecho que tienen todas las personas a conocer, actualizar y rectificar todo tipo de información que se encuentre en tratamiento dentro de una base de datos. A condición de que la autorización o la autodeterminación informática, es el referente medular de mayor importancia en el derecho al habeas Data, ya que permite a los titulares garantizar efectivamente su Derecho.

Que con base al análisis dinámico realizado y a lo largo de 20 años de ejercicio del Derecho a la Protección de Datos Personales, se ha mantenido en una línea jurisprudencial bien definida, la cual reconoció que para el tratamiento de datos personales, es indispensable la autorización explicita del titular de los datos y que la misma no podrá ser tacita, ya que debe cumplir con todas las cualificaciones del consentimiento, es decir, debe ser libre, previa y expresa.

Hecha esta salvedad, con base al análisis estático de la sentencia C748 de 2011, se puedo concluir que aún en la actualidad y sin importar la finalidad con la que vayan a ser tratados lo datos, debe existir la autorización expresa del titular de los datos o se exceptúan aquella, ya sea, mediante orden legal o judicial.

Dicho lo anterior y en referencia a los datos biométricos, señalo que en el caso particular no dicha hipótesis no se enmarca dentro de los literales b,c,d y e por lo cual se

Aún podemos precisar que de acuerdo a la jurisprudencia de la Corte Constitucional, lo establecido en la Constitución Política, la Ley Estaturia No. 1581 de 2.012 y sus decretos reglamentarios, la autorización o la autodeterminación informática es considerada como el "pilar fundamental del habeas data," la cual debe ser libre, previa y expresa o exceptuada

mediante un expreso mandato legal o mediante una orden de una autoridad judicial y sin ella se lesiona en directo el Derecho Fundamental a la Protección de Datos Personales.

Sin más preámbulo, citando a la Superintendencia de Industria y Comercio, como entidad reguladora y protectora por el cumplimiento y bienestar del habeas data, se sostuvo que de acuerdo a la Ley E. 1581 de 2012 y al Decreto 1377 de 2013 y en consonancia con lo propuesto por Alexy (2014) la norma que se sustrae de dicho enunciando resalta que: Se encuentra prohibido el tratamiento de datos sensibles a excepción de lo contemplado en el artículo 6º de la ley 1581 -que veremos a continuación- y que los responsables deberán cumplir 2 obligaciones a la hora de tratar datos de naturaleza sensible: (i) informar la no obligación de autorizar su tratamiento y (ii) obtener su consentimiento expreso. Lo anterior, a no ser que, se cumplan con las excepciones contempladas en el artículo 6 las cuales son:

"a) El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización; b) El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización; c) El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular; d) El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; e) El Tratamiento tenga una finalidad histórica, estadística o científica. En este

evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares."

Así que, para el caso de las cámara de vídeo vigilancia, las excepciones enmarcadas en los literales b,c,d y e no se cumplen, por lo que se debe enmarcar en el literal a. Siempre y cuando no se entienda que para el tratamiento de datos sensibles es valida la autorización a través de conductas inequívocas.

Llegados a este punto, se considera que las cámaras de seguridad son demasiado invasivas e intrusivas para el desarrollo de la intimidad o privacidad en conexión con la dignidad humana.

También se concluye que la tecnología avanza de manera más ágil que el brazo legislativo y a su vez abre paso a nuevos caminos inexplorados para el derecho y según la dogmática constitucional, ningún derecho fundamental es absoluto, por lo tanto, el derecho fundamental a la protección de datos personales encuentra colisión –o como dice el Autor Robert Alexy (2014), encuentra tensión- frente a bienes o intereses individuales o colectivos como la seguridad nacional y/o personal. Pero que aún con la existencia de la tensión, será necesario llevar a cabo el principio de proporcionalidad o ponderación, que comprende: el principio de idoneidad si el medio que se utiliza es objetivo con el fin propuesto; el principio de necesidad hace alusión, a que no exista otro medio que afecte en menor medida las garantías fundamentales de los ciudadanos y el juicio de proporcionalidad en sentido estricto, es que se aplique una ponderación equilibrada que entregue más beneficios que desventajas para el interés general.

Finalmente, el desconocimiento de los ciudadanos y de la sociedad, permitió la instalación masiva de cámaras en todo Colombia y como lo corrobora el sitio web

insecam.org, todos estamos expuestos a la entrega deliberada de datos y más allá a la perdida de la privacidad. Se recuerda que si los datos son incluidos sin cumplir con la autorización expresa, exigencia demarcada a lo largo del presente trabajo, los responsables deberán borrar inmediatamente la información, ya que se constituye una violación del debido proceso en el acopio del dato, como también la vulneración directa del derecho fundamental al habeas data.

Bibliografía

Alexy, R. (2014). Teoría de los derechos fundamentales. Segunda Edición, Madrid: Centro de estudios políticos y constitucionales,

Álvarez Padilla y Garzón Muñoz, D. J. (2009). Proveedores de servicios de Internet y de contenidos, responsabilidad civil y derechos de autor. Studiositas, edición diciembre, 51-64.

España, Agencia Española de Protección de Datos (2014), *Guía de Videovigilancia.*

Colombia, Congreso Nacional de la República, (17 de Octubre de 2012). Ley Estatutaria No. 1581 de 2012 "*Por la cual se dictan disposiciones generales para la protección de datos personales."* Bogotá.

Colombia, Corte Constitucional, *"Sentencia T 414 de 1992"* M.P. Dr. Ciro Angarita, Bogotá

Colombia, Corte Constitucional, "*Sentencia T 022 de 1993"* M.P. Dr. Ciro Angarita Baron, Bogotá.

Colombia, Corte Constitucional, *"Sentencia SU 082 de 1995"* M.P. Dr. Jorge Arango Mejía, Bogotá

Colombia, Corte Constitucional, *"Sentencia T-729 de 2002"* M.P. Dr. , Bogotá

Colombia, Corte Constitucional *"Sentencia T-310 de 2003"* M.P. Dr. Clara Inés Vargas, Bogotá

Colombia, Corte Constitucional, "*Sentencia C 431 de 2003"* M.P. Dr. Alfredo Beltrán Sierra. Bogotá

Colombia, Corte Constitucional, *"Sentencia C 1011 de 2008"* M.P. Dr. Jaime Cordoba Triviño, Bogotá

Colombia, Corte Constitucional, *"Sentencia C 748 de 2011"* M.P. Dr. Jorge Ignacio Pretelt Chaljub, Bogotá

Colombia, Constitución Política de 1991.

Colombia, Presidente de la República de Colombia, (27 de Junio de 2013). Decreto 1377 de 2013, "*Por el cual se reglamenta parcialmente la ley 1.581 de 2.012."*

Colombia,Superintendencia de industria y comercio (2012), Oficina Jurídica, Concepto No. 12-185526-00001 de 4 de Diciembre

Colombia, Superintendencia de industria y comercio (2013), Oficina Jurídica, Concepto No. 13-123335-00001 de 9 de Julio

Consejo Europeo, Resolución 509 (1968)"*Los Derechos humanos y los nuevos logros científicos y técnicos*"

Convención Americana sobre Derechos Humanos (1969). Recuperado de: www.oas.org/Juridico/spanish/tratados/b-32.html

Convenio para la Protección de los Derechos y Libertades Fundamentales, Recuperado de: www.acnur.org/biblioteca/pdf/1249.pdf

Declaración Universal de los Derechos del Hombre, Recuperado de: www.un.org/es/documents/udhr/

Diccionario educativo inicial larousse, (2003) Editorial ultra S.A. de C.V. México P. 45.

Europa, Convenio para la protección de los derechos y las libertades fundamentales (1956), Recuperado de: http://www.echr.coe.int/Documents/Convention_SPA.pdf

Instituto Nacional de Estándares y tecnología. (Septiembre de 2011) Obtenido de http://www.nist.gov/

López Medina, D. E. (2006). El derecho de los Jueces. Bogotá: Segunda Edición Legis S.A.

López Medina, D. E. (2012). Teoría impura del derecho. Colombia: Legis S.A.

López Rodríguez Julio César. (2007) "Estructura, funcionamiento y aplicación de las cámaras IP. Recuperado de http://dgsa.uaeh.edu.mx:8080/bibliotecadigital/bitstream/handle/231104/1747/Estructura,%20funcionamiento%20y%20aplicación%20de%20las%20cámaras%20IP.pdf?sequence=1&isAllowed=y

Mendoza, O. F. (2014). El derecho a la autodeterminación informativa en la era de la llamada videovigilancia en el sector privado en México. Una perspectiva desde la ley federal de protección de datos personales en posesión de particulares y los retos pendientes. Revista de Derecho, Comunicaciones y Nuevas Tecnologías No. 12, Julio - Diciembre de 2014. ISSN 1909-7786

OECD, O. p. (1980). Directrices. Recuperado de: http://www.oecd.org/sti/ieconomy/15590267.pdf

Organización de las Naciones Unidas (ONU), Declaración Universal de los derechos humanos, Recuperado de: http://www.un.org/es/documents/udhr/

Organización de las Naciones Unidas (ONU), pacto internacional de derechos civiles y políticos (1976), recuperado de: http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx

Organización de las Naciones Unidas (ONU), *la resolución No. 3384* (1975) "*Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad*"

Orwell, George (1949), *Gran hermano o 1984,* Recuperado de: http://antroposmoderno.com/word/George_Orwell-1984.pdf

Quinche. R (2.014) El precedente judicial y sus reglas, editorial Legis S.A.

Diccionario de la Real Academia de la Lengua Española (RAE) (2016), Disponible en: http://www.rae.es

Remolina, N. (2013) Tratamiento de datos personales "Aproximación internacional y comentarios a la Ley 1581 de 2012, editorial Legis S.A.

Remolina Nelson y Gómez Ana, en Derecho y Tic 10.0, editorial Temis S.A. 2014

Sitio web, Insecam - World biggest online cameras directory, Disponible en http://www.insecam.org

Anexos

<table>
<tr><td colspan="6">ANALISIS JURISPRUDENCIAL</td></tr>
<tr><td colspan="3">Nombre Alumno: EDWARD ANDRES BELTRAN LOPEZ</td><td colspan="3">Materia: MONOGRAFIA DE GRADO</td></tr>
<tr><td>ORIGEN</td><td>Corte Constitucional</td><td>RADICACION</td><td>SENTENCIA C 748 DE 2011</td><td>PONENTES :</td><td>JORGE IGNACIO PRETELT CHALJUB</td></tr>
<tr><td>Tipo de acción</td><td>C</td><td colspan="4">Tipo de decisión: CONTROL DE CONSTITUCIONALIDAD DE LOS PROYECTOS DE LEY ESTATUTARIA</td></tr>
<tr><td>Normatividad Aplicable</td><td colspan="5">ARTÍCULO 15 DE LA CONSTITUCIÓN POLÍTICA DE COLOMBIA</td></tr>
<tr><td>Precedente</td><td colspan="5">LA AUTORIZACIÓN ES CONSIDERADA EL ASPECTO MEDULAR EN EL TRATAMIENTO DE DATOS PERSONALES, LA CUAL DEBERÁ TENER LAS CUALIFICACIONES DEL CONSENTIMIENTO, ES DECIR, DEBE SER LIBRE, PREVIA Y EXPRESA.</td></tr>
<tr><td>Tema</td><td colspan="5">HABEAS DATA Y PROTECCIÓN DE DATOS PERSONALES</td></tr>
<tr><td>Subtemas</td><td colspan="5">LA AUTORIZACIÓN O LA AUTODETERMINACIÓN INFORMATIVA</td></tr>
<tr><td>Hechos Relevantes</td><td colspan="5">En términos generales el trámite legislativo del proyecto de ley estatutaria de habeas data y protección de datos personales, cumplió con los requisitos constitucionales previstos para cualquier decisión legislativa y particularmente para este tipo de leyes de especial jerarquía, pues habiendo sido presentado ante el Congreso y su texto junto con la exposición de motivos publicada oportunamente, su aprobación, que tuvo inicio en la comisión primera de la Cámara de Representantes, se efectuó dentro de una sola legislatura; se cumplieron los debates en las comisiones permanentes y plenarias de ambas cámaras legislativas; se publicaron las ponencias junto con los pliegos modificatorios y se dio cumplimiento a los anuncios previos para discusión y aprobación.</td></tr>
</table>

Pregunta Problemita:	¿Hay violación del Derecho a la protección de datos personales (artículo 15. C.P.) Cuando cámaras de videovigilancia recaban datos personales sin autorización del titular?

ANALISIS CONCRETO

Análisis concreto(Obiter dicta)

El derecho a la intimidad fue reconocido por primera vez en 1948, en la Declaración Universal de los Derechos Humanos, cuyo artículo 12 dispone que toda persona debe ser protegida contra injerencias arbitrarias en su vida privada, familia, domicilio o correspondencia, así como de ataques contra su honra y reputación.[2] Posteriormente, en 1966, este precepto fue reproducido por el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), con lo cual se le dio naturaleza vinculante entre los estados partes.

En 1983, una sentencia del Tribunal Constitucional alemán denominó por primera vez el derecho a la protección de los datos personales como **derecho a la autodeterminación informativa**, con fundamento en el derecho al libre desarrollo de la personalidad.[8] Para este tribunal, tal derecho comprende la facultad de decidir por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida. Además, el tribunal señaló que la garantía del derecho requiere especiales medidas de protección, teniendo en cuenta que la interconexión de varias bases de datos puede dar lugar a la elaboración de un perfil de la personalidad que limite la libertad de decisión. Este ejemplo fue seguido por el Tribunal Constitucional español, el cual, en 1993, precisó que el artículo 18.4 de la constitución española consagra un derecho fundamental autónomo al disponer que la ley debe limitar el uso de la informática para garantizar la intimidad, el honor y el pleno ejercicio de los derechos de los ciudadanos.

La configuración de la autodeterminación informativa como derecho autónomo inicia con la sentencia T 414 de 1992, donde el Magistrado Ponente y considerado padre del Derecho al Habeas Dr. Ciro Engarita Barón, reconoce que toda persona tiene derecho a controlar su información personal, incluyendo por primera vez una cláusula integradora que expresa: En todos los otros casos similares a los hechos fácticos de esta sentencia se deberá seguir las reglas aquí impuestas, reconociendo el Derecho a la Protección de Datos Personales.

Argumentos que sustentan la decisión y sus precedentes (Ractiodecidendi)

• “Los Datos Personales Deben Ser Procesados Con Un Propósito Específico Y Explícito. En Ese Sentido, La Finalidad No Sólo Debe Ser Legítima Sino Que La Referida Información Se Destinará A Realizar Los Fines Exclusivos Para Los Cuales Fue Entregada Por El Titular. Por Ello, Se Deberá Informar Al Titular Del Dato De Manera Clara, Suficiente Y Previa Acerca De La Finalidad De La Información Suministrada Y Por Tanto, No Podrá Recopilarse Datos Sin La Clara Especificación Acerca De La Finalidad De Los Mismos.”

• “El Principio De Libertad, Pilar Fundamental De La Administración De Datos, Permite Al Ciudadano Elegir Voluntariamente Si Su Información Personal Puede Ser Utilizada O No En Bases De Datos. También Impide Que La Información Ya Registrada De Un Usuario, La Cual Ha Sido Obtenida Con Su Consentimiento, Pueda Pasar A Otro Organismo Que La Utilice Con Fines Distintos Para Los Que Fue Autorizado Inicialmente.

• Para Que Exista Una Vulneración Del Derecho A La Protección De Datos Personales, “Debe Desconocerse Alguno De Los Tres Aspectos Enunciados. Es Decir, La Información Contenida En El Archivo Debe Haber Sido Recogida De Manera Ilegal, Sin El Consentimiento Del Titular Del Dato (I), Ser Errónea (Ii) O Recaer Sobre Aspectos Íntimos De La Vida De Su Titular No Susceptibles De Ser Conocidos Públicamente (Iii). Por El Contrario, El Suministro De Datos Veraces, Cuya Circulación Haya Sido Previamente Autorizada Por Su Titular, No Resulta, En Principio, Lesiva De Un Derecho Fundamental.

• Si El Dato Sensible Es Tratado Sin Autorización Del Titular, Bien Sea Porque Es Requerido Por Una Ley O Por Las Limitantes Expuestas Aquí, “Siempre Y Cuando Se Entienda, Como Se Mencionará Más Adelante, Que Tal Autorización, Además De Estar Contenida En Una Ley, Sea Conforme A Las Garantías Que Otorga El Habeas Data, Por Ejemplo En Materia De Finalidad, Y Cumpla Las Exigencias Del Principio De Proporcionalidad.”

• **La Autodeterminación Informática Es La Facultad De La Persona A La Cual Se Refieren Los Datos, Para Autorizar** Su Conservación, Uso Y Circulación, De Conformidad Con Las Regulaciones Legales.” Esa Posición Ha Sido Reiterada, Entre Muchas Otras, En Las Sentencias T-580 De 1995, T-448 De 2004, T-526 De 2004, T-657.

•El Consentimiento Es Un Aspecto **Medular Del Derecho Al Habeas Data.**“El Tratamiento Sólo Puede Ejercerse Con El Consentimiento, Previo, Expreso E Informado Del Titular. Los Datos Personales No Podrán Ser Obtenidos O Divulgados Sin Previa Autorización, O En Ausencia De Mandato Legal O Judicial Que Releve El Consentimiento.

Parte Resolutiva
Primero.- Declarar **Exequible** Por Su Aspecto Formal, El Proyecto De Ley Estatutaria No. 046/10 Cámara – 184/10 Senado "Por La Cual Se Dictan Disposiciones Generales Para La Protección De Datos Personales"; Declarar **Exequibles** Los Artículos 1, 2, 3, 4, 5, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 21, 22, 24, 25, 28, 32, 33 Y 34 Del Proyecto De Ley, De Conformidad Con Lo Expuesto En La Parte Motiva De Esta Providencia; Declarar **Exequible** El Artículo 8 Del Proyecto De Ley Objeto De Revisión, Excepto La Expresión "*Sólo*", Del Literal E) Que Se Declara **Inexequible.**
Conclusiones
Como Conclusiones Se Obtienen, Que La Autorización En El Derecho A La Protección De Datos Personales, Es Considerada El Aspecto Medular Para Poder Realizar El Tratamiento De La Información Personal, También Se Concluye Que El Acopio De Información Sin La Debida Autorización Vulnera En Concreto El Derecho Fundamental Y Toda Captura Y Tratamiento De Información Personal Sin El Debido Consentimiento Será Ilegal.

Nombre quien realiza análisis	EDWARD ANDRÉS BELTRÁN LÓPEZ