

HERRAMIENTAS JURÍDICAS PARA LA PROTECCIÓN DE LOS DATOS
PERSONALES EN COLOMBIA: ANÁLISIS DEL GRADO DE PROTECCIÓN JURÍDICA
DEL HABEAS DATA.



Presentado por
CAMILO JOSÉ PUELLO RINCÓN

UNIVERSIDAD LIBRE SECCIONAL CUCUTA
FACULTAD DE DERECHO, CIENCIA POLÍTICA Y SOCIALES
CÚCUTA, COLOMBIA

2016

HERRAMIENTAS JURÍDICAS PARA LA PROTECCIÓN DE LOS DATOS
PERSONALES EN COLOMBIA: ANÁLISIS DEL GRADO DE PROTECCIÓN JURÍDICA
DEL HABEAS DATA.



Presentado por
CAMILO JOSÉ PUELLO RINCÓN

Proyecto de grado presentado como requisito parcial para optar al título de abogado

Directora
CINDY CHARLOTTE REYES SINISTERRA
Abogada

Asesor metodológico
LUIS ENRIQUE NIÑO OCHOA
Especialista en Investigación Social

UNIVERSIDAD LIBRE SECCIONAL CUCUTA
FACULTAD DE DERECHO, CIENCIA POLÍTICA Y SOCIALES
CÚCUTA, COLOMBIA
2016



**UNIVERSIDAD LIBRE DE COLOMBIA
SECCIONAL CÚCUTA
BIBLIOTECA “MANUEL JOSÉ VARGAS DURÁN”**

RESUMEN – TRABAJO DE GRADO

CAMILO JOSÉ PUELLO RINCÓN

AUTOR(ES) NOMBRES Y APELLIDOS COMPLETOS

Derecho, Ciencias Políticas y Sociales

FACULTAD

Cindy Charlotte Reyes Sinisterra

DIRECTOR

**HERRAMIENTAS JURÍDICAS PARA LA PROTECCIÓN DE LOS DATOS PERSONALES EN COLOMBIA:
ANÁLISIS DEL GRADO DE PROTECCIÓN JURÍDICA DEL HABEAS DATA**

TÍTULO

RESUMEN

La presente investigación aborda de manera novedosa el análisis del nivel de protección presente en las herramientas creadas para proteger al uso indebido de datos personales por medio de nuevas tecnologías de la información y las comunicaciones.

Después de la identificación del proyecto, la formulación del problema a tratar y los objetivos a cumplir, se expone el marco referencial, compuesto en el espacio internacional por el antecedente teórico encontrado en investigaciones previas que han indagado acerca de los mecanismos de protección de datos personales, y en el espacio nacional, los estudios del nivel de protección que otorga la norma sustancial, en especial la ley 1266 de 2008, esfuerzo realizado por el profesor Nelson Remolina como parte de su investigación para optar por el título de Doctor en Derecho en la Pontificia Universidad Javeriana; también se han encontrado proyectos de grado que han sumado un aporte fructífero al centrar su análisis en algunas de las herramientas jurídicas como la investigación sobre las sanciones proferidas por la Superintendencia de Industria y Comercio, que es autoridad de protección de datos personales, y la comparación de la legislación penal informática colombiana con la vigente en España, estas últimas investigaciones realizadas en la Universidad Libre Seccional Cúcuta.

Esta es una investigación jurídica acerca de las normas vigentes del ordenamiento colombiano sobre las herramientas que protegen el habeas data, describiendo las características y rasgos importantes de estas a partir del análisis de la ley y los estudios doctrinales o sentencias judiciales que ayudan en la comprensión completa de ellas de manera sistemática.

Esta investigación comienza con el análisis los orígenes filosóficos y jurídicos que sustentan la existencia del derecho fundamental de habeas data. El principal fundamento son postulados del liberalismo y su concepción de ser humano como ser libre, autónomo y digno para comprender la justificación de proteger y garantizar del buen uso del dato personal actualmente.

Hecho lo anterior es factible comprender como ha sido desarrollado en el contexto colombiano la regulación jurídica: de un nulo reconocimiento como derecho fundamental autónomo al ser parte de la privacidad a la consagración de su independencia jurídica con su reconocimiento constitucional y la creación de mecanismos específicos de protección para su garantía que se analizan detalladamente y se exponen serios reparos en el diseño de algunos de ellos. Poniéndose al día de las transformaciones jurídicas y sociales que ocurrieron durante el siglo XX: surgimiento de estado social de derecho, constitucionalización del derecho, globalización y revolución de las TIC.

Luego de comprendido cual ha sido el desarrollo histórico jurídico del derecho fundamental de tratamiento debido de datos personales se entra a enunciar, a partir de la desintegración del objeto de protección del derecho de habeas data, cuales son los derechos y que mecanismos pueden protegerlos según el ordenamiento jurídico colombiano. Así como también la conexidad o colisión con otros derechos fundamentales. Comprendiendo que tiene la misma estructura de los otros derechos fundamentales se identifican que es un derecho instrumental compuesto de los derechos que se denominan derechos ARCARS: Autorizar, Revocar, Conocer, Actualizar, Rectificar y Suprimir toda información que infrinja los principios adecuados para el debido tratamiento de datos personales.

Por último se expone el aporte fundamental de esta investigación que es el nivel de protección jurídico de las herramientas, realizado a partir de la toma de recomendaciones que realizó la Unión Europea para evaluar el nivel adecuado de protección de los ordenamientos externos a los países miembros, así como también el intento de sintetizar unos principios comunes a los modelos vigentes de protección de datos personales. Identificando de esta manera la existencia de unos requisitos mínimos para obtener el nivel adecuado y luego valorando, mediante el análisis del grado de protección jurídica, que los aspectos por modificar en las herramientas para la protección del habeas data en Colombia para alcanzar el nivel adecuado que representaría una oportunidad de apertura de negocios extranjeros de tecnología de la información que usan intensivamente los datos personales, como bien lo quiere hacer el Gobierno Nacional para promover el desarrollo del país.

CARACTERÍSTICAS:

PÁGINAS: _____ PLANOS: _____ ILUSTRACIONES: _____ CD-ROM: _____

ANEXOS: _____



San José de Cúcuta, Junio 15 de 2016

Doctor:
DIEGO ARMANDO YAÑEZ MEZA
Director
Centro Seccional de Investigaciones
Universidad Libre de Colombia
Cúcuta

Ref. Aprobación disciplinar del proyecto

Cordial saludo

Por medio de la presente expreso la APROBACIÓN DISCIPLINAR del Proyecto de Grado titulado HERRAMIENTAS JURÍDICAS PARA LA PROTECCIÓN DE LOS DATOS PERSONALES EN COLOMBIA: ANÁLISIS DEL GRADO DE PROTECCIÓN JURÍDICA DEL HABEAS DATA; propuesto por el estudiante CAMILO JOSÉ PUELLO RINCÓN, concódigo 1.090.463.804 del Quinto año de Derecho diurno grupo GL de la Universidad Libre Seccional Cúcuta.

Sin otro particular me suscribo de Usted.

Atentamente

CINDY CHARLOTTE REYES SINISTERRA

Abogada

Especialista en Derecho Procesal

TP: 221.871 del C.S.J.



San José de Cúcuta, Junio 15 de 2016

Doctor:
DIEGO ARMANDO YAÑEZ MEZA
Director
Centro Seccional de Investigaciones
Universidad Libre de Colombia
Cúcuta

Ref. Aprobación metodológica del Proyecto de Grado

Cordial saludo

Por medio de la presente expreso la APROBACIÓN METODOLOGICA del Proyecto de Grado titulado HERRAMIENTAS JURÍDICAS PARA LA PROTECCIÓN DE LOS DATOS PERSONALES EN COLOMBIA: ANÁLISIS DEL GRADO DE PROTECCIÓN JURÍDICA DEL HABEAS DATA; propuesto por el estudiante CAMILO JOSÉ PUELLO RINCÓN con código 1.090.463.804 del Quinto año de Derecho diurno grupo GL de la Universidad Libre Seccional Cúcuta.

Sin otro particular me suscribo de Usted.

Atentamente

LUIS ENRIQUE NIÑO OCHOA
Especialista en Investigación Social – UIS
Docente – Investigador
Universidad Libre

UNIVERSIDAD LIBRE SECCIONAL CÚCUTA
FACULTAD DE DERECHO, CIENCIA POLÍTICA Y SOCIALES

NOTA DE ACEPTACIÓN

Presidente del jurado

Jurado

Jurado

San José de Cúcuta, juniode 2016

“Probablemente solo tengamos la oportunidad de hacer
unas cuantas cosas que de verdad
sean excepcionales y de hacerlas bien.
Creo que si algo te sale bien entonces
debes hacer otra cosa igual de maravillosa.
no te quedes demasiado tiempo en lo mismo.
Decide qué es lo que sigue”
STEVE P. JOBS

"Cuando me dejo llevar por lo que soy, me convierto en lo que podría ser."
Lao Tzu

Hace 23 años tuvimos nuestro primer mejor momento.
Ahora es el segundo mejor momento.
A mis padres quiero dedicarles
este pequeño trabajo

AGRADECIMIENTOS

El autor expresa sus agradecimientos a:

Cindy Charlotte Reyes Sinisterra, Asesora Disciplinar del Trabajo de Grado, por el gran ejemplo académico.

Luis Enrique Niño Ochoa, Asesor Metodológico del Trabajo de Grado, por su valiosa orientación, paciencia y aliento para finalizarlo con satisfacción.

RESUMEN EJECUTIVO

Camilo José Puello Rincón, estudiante de la Universidad Libre de Colombia seccional Cúcuta, presenta el trabajo de grado, como requisito parcial para optar el título de abogado, titulado “Herramientas jurídicas para la protección de datos personales en Colombia. Análisis del grado de protección jurídica del Habeas Data”. La presente investigación aborda de manera novedosa el análisis de las herramientas creadas para proteger a todas las personas del impacto negativo que puedan tener las nuevas tecnologías de la información y las comunicaciones en nuestros usos cotidianos. Después de la identificación del proyecto, la formulación del problema a tratar y los objetivos a cumplir, se expone el marco referencial, compuesto por el antecedente teórico encontrado en investigaciones previas, que han indagado acerca de los mecanismos de protección de datos personales a nivel internacional; en el espacio nacional, los estudios del nivel de protección que otorga la norma sustancial, en especial la ley 1266 de 2008, esfuerzo realizado por el profesor Nelson Remolina como parte de su investigación para optar por el título de Doctor en Derecho en la Pontificia Universidad Javeriana; también se han encontrado proyectos de grado que han sumado un aporte fructífero al centrar su análisis en algunas de las herramientas jurídicas como la investigación sobre las sanciones proferidas por la Superintendencia de Industria y Comercio, que es autoridad de protección de datos personales, y la comparación de la legislación penal informática colombiana con la vigente en España, estas últimas investigaciones realizadas en la Universidad Libre Seccional Cúcuta. Seguidamente, se desarrollan las bases teóricas en primera medida, se estudia la teoría del liberalismo desde una perspectiva filosófica, retomando los postulados Lockianos, sobre todo la teoría de la resistencia que es el germen de los derechos humanos actuales y recientemente del derecho del habeas data reconocido internacionalmente; en segundo lugar se expone la necesidad de entender los derechos humanos de manera histórica, vinculado a los acontecimientos socio-históricos más importantes de la historia moderna y contemporánea, para aterrizar con esta comprensión contextual en la justificación del surgimiento de los derechos fundamentales y el interés de protegerles a través de una garantía efectiva que repare los daños causados por el estado; en tercer lugar se expone la importancia de la teoría de la responsabilidad civil como soporte teórico para sustentar la necesidad de una reparación frente a la vulneración del habeas data; en último lugar el derecho al habeas data en su teoría

fundacional, que se apoya en los postulados de la libertad, de la protección estatal para un goce efectivo, dada la pertenencia a la misma dignidad humana, y en la reparación por los perjuicios causados cuando se la vulnera, haciendo de este derecho una importante fuente de libertad en las actuales circunstancias donde pasamos a ser una sociedad tecno-informática que requiere del uso de datos personales para poder gozar de muchos beneficios. Posteriormente en el tercer capítulo, se señala el diseño metodológico que enmarca que tipo de investigación es esta y el método de análisis que se aplicó a la información para estructurar la misma: es **jurídica** al centrarse en las normas vigentes del ordenamiento colombiano sobre las herramientas que protegen el habeas data, **descriptiva** porque se especifican las características y rasgos importantes de estos a partir del análisis de la ley y los estudios doctrinales pertinentes. En el cuarto capítulo se entra a desarrollar los objetivos específicos de la investigación, el primero que describe las herramientas jurídicas de protección, previo análisis corto de los orígenes filosóficos y jurídicos que sustentan la existencia del derecho fundamental de habeas data, el segundo dedicado a enunciar, a partir de la desintegración del objeto de protección del derecho de habeas data, cuales son los derechos y que mecanismos pueden protegerlos; por último, el tercer objetivo se centra en analizar el nivel de protección jurídico de las herramientas y la incidencia de los problemas, encontrados al revisar su estructuración, en la efectividad de la protección del habeas data. Finalmente se procede a exponer las conclusiones de la investigación.

CONTENIDO

AGRADECIMIENTOS.....	viii
INTRODUCCIÓN.....	1
IDENTIFICACION DEL PROYECTO	4
Título	4
Planteamiento del problema	4
Formulación del problema.....	6
Sistematización del problema.....	6
Justificación.....	6
Objetivos	7
<i>Objetivo general</i>	7
<i>Objetivos específicos</i>	8
MARCO DE REFERENCIA	9
Antecedentes	9
Bases teóricas	10
<i>Teoría del liberalismo</i>	10
<i>Teoría de los derechos fundamentales</i>	13
<i>Teoría de los derechos humanos</i>	18
<i>Teoría de la responsabilidad civil</i>	20
<i>Habeas Data - protección de datos</i>	25
Bases legales.....	34
Sistema teórico	54
<i>Definición de variables</i>	54
Operacionalización de variables	56
DISEÑO METODOLÓGICO	58
Tipo y método de investigación.....	58
Población y muestra	59
Análisis de información.....	60
Análisis documental	60
Análisis de guía análisis jurisprudencial.....	110
HERRAMIENTAS JURÍDICAS PARA LA PROTECCIÓN DE LOS DATOS PERSONALES EN COLOMBIA: ANÁLISIS DEL GRADO DE PROTECCIÓN JURÍDICA DEL HABEAS DATA	141
Herramientas jurídicas para la protección de datos personales en Colombia	141
<i>Origen del derecho al Habeas Data en el Principio General de la Libertad</i>	141
<i>Derecho de Protección del Dato Personal y el Habeas Data</i>	174
<i>Justificación para la protección jurídica con herramientas específicas</i>	208
<i>Herramientas jurídicas para la protección de datos personales en Colombia</i>	222

Derechos del Habeas Data que garantizan los mecanismos para la protección de datos personales en Colombia	273
<i>Objeto de protección constitucional del derecho de protección de datos personales</i>	274
<i>Estructura del derecho fundamental a la protección de datos personales según su desarrollo legal</i>	279
<i>Derechos protegidos por los mecanismos</i>	303
<i>Colisiones de derechos fundamentales</i>	316
Nivel de Protección jurídica ante la vulneración del Habeas Data en Colombia, frente a los modelos europeo y norteamericano.	319
<i>Estándares Internacionales aplicables al tratamiento de datos personales: Dos modelos de referencia</i>	320
<i>Requisitos para un nivel adecuado de protección jurídica</i>	330
<i>Análisis del grado de protección jurídica de los mecanismos de protección frente a los estándares internacionales</i>	341
CONCLUSIONES Y RECOMENDACIONES	349
REFERENCIAS BIBLIOGRÁFICAS	361
ANEXOS	368

INTRODUCCIÓN

“Tan pronto como se opta
por un determinado camino,
aparecen nuevos senderos que
obligan a decidir sobre el itinerario”

Ernesto Benda,
*Capítulo X. El Estado Social de Derecho*¹

El advenimiento del siglo XX representó la aparición de nuevas formas de perversión humana nunca vistas, pero también inició el proceso de masificación e industrialización más grande de la historia, que permitió el crecimiento económico suficiente para que una gran cantidad de personas disfrutasen de niveles de vida antes no vistos y tuviesen un mayor empoderamiento político. El estado intenta ser garante y representativo de las nuevas tendencias ideológicas que van surgiendo, mientras que la tecnología extiende los horizontes del entendimiento humano, de la realidad y de sus congéneres.

En 1945 fue el año del fin de la Segunda Guerra Mundial, pero también es el año que inicia el crecimiento de la sociedad capitalista, la globalización de la información, la expansión mundial de las nuevas formas de economía y la imbricación de la tecnología en la vida cotidiana. Los ciudadanos piden el fortalecimiento del Estado ante la más despiadada dictadura del interés lucrativo que colisiona con la realización de los derechos fundamentales, al mismo tiempo que piden mejores condiciones económicas.

Más de tres mil millones de personas que acceden a la internet están expuestas a la recolección de datos personales para acceder a los servicios web, al hacer esto su libertad es amenazada desde múltiples flancos: a los grupos de poder gubernamentales, que actúan en su propio interés o de manera despótica, suman ahora los grupos privados de la sociedad, que intentan obtener normas favorables o laxas con una desprotección de los derechos fundamentales. Frente a lo cual la sociedad reacciona promoviendo instrumentos jurídicos que

¹En Mainhoffer, Benda, Hesse, Vogel y Heyde. Manual de derecho Constitucional. Madrid: Tecnos.

permitan conservar la tutela jurídica de los derechos civiles y sociales, así como también el surgimiento de nuevos derechos garantía de los anteriores, que tutelan aspectos de la realidad humana totalmente impensados.

En esta sociedad que utiliza la tecnología como herramienta para la vida, se busca evitar que el hombre no sea convertido en un hombre unidimensional que sólo provee información y se le entregan servicios, como autómatas consumidores despersonalizados, pese a que se alegue la recolección de información como necesaria para ofrecer un buen servicio. Este es el contexto en el cual se presentan los resultados de este proyecto de investigación.

La masificación de la tecnología y la preocupación por proteger los derechos fundamentales que puedan verse afectados inciden en la configuración de un derecho fundamental reconocido con el nombre de “habeas data”. Las herramientas jurídicas de protección de este derecho surgieron de Europa y se expandieron a todo el mundo. Colombia no fue la excepción y en una reciente ley (1581 de 2012) estableció un régimen general de protección de datos personales que pretende cumplir con el deber constitucional encargado al legislador por el constituyente primario de 1991. Es importante conocer el nivel de protección jurídica que tienen las herramientas para comprender si ofrecen una tutela jurídica efectiva del derecho de habeas data.

En el primer capítulo de esta investigación se trazan los aspectos que dieron origen a la misma: se expone el título de la investigación; el planteamiento del problema está centrado en la preocupación por obtener la protección del habeas data a través de la herramienta más adecuada; la formulación del problema es la materialización precisa para comenzar a indagar sobre lo planteado en el problema que desmenuzan en tres interrogantes a resolver cuando se les formula como objetivos.

En el segundo capítulo se exponen los antecedentes de la investigación, resaltando estudios doctrinales sobre los mecanismos de protección jurídica y el análisis del nivel de protección jurídica de la ley anterior a la 1581 de 2012 sobre protección de datos personales y luego el fundamento teórico de la investigación sustentado en los orígenes liberales del

derecho fundamental de habeas data y la consciencia de necesidad de la existencia de herramientas para su tutela adecuada, teniendo el vínculo por medio de la Constitución que impone el deber al Estado y las autoridades públicas.

En el tercer capítulo se expone cual fue el diseño metodológico adoptado. Se destaca el hecho de ser una investigación centrada en el ordenamiento jurídico vigente, en lograr a través de su análisis la detección de las características que tienen las herramientas jurídicas y ayudado del estudio documental acerca de lo que ha producido la doctrina en sus reflexiones sobre el habeas data, se comprende mucho mejor el diseño y regulación de los mismos. Por esta razón la investigación es jurídica-descriptiva, su método de investigación es la analítica sistemática y mental, usando la técnica de investigación documental para plasmar el análisis de las ideas de los estudios y la jurisprudencia sobre el tema.

En el cuarto capítulo se presentan los desarrollos de la investigación en tres partes. La primera parte empieza con una corta exposición acerca del origen del derecho al habeas data, su configuración como derecho fundamental y los argumentos que dan justificación actual para su existencia como son la protección de la dignidad humana ante el avance de las nuevas tecnologías sobre cada persona mediante el reconocimiento de nuevas facultades jurídicas para evitar o detener la intromisión en nuestra vida y el uso de la información que conocen de cada uno, por último se centra en la descripción característica de las herramientas que rigen el ordenamiento jurídico colombiano. En la segunda parte se expone la estructura del derecho fundamental al habeas data en el ordenamiento jurídico colombiano, su desarrollo jurisprudencial, cuales derechos se encuentran protegidos por las herramientas jurídicas y las colisiones con otros derechos fundamentales. En la tercera parte, se analiza el nivel de protección jurídica de las herramientas, para ello se comienza por el análisis de los dos estándares internacionales, seleccionando el examen de protección que tiene el estándar europeo de protección de datos personales para indagar sobre el nivel de protección jurídica debido a la profunda influencia que ejerció en la ley estatutaria de protección de datos personales vigente en Colombia.

IDENTIFICACION DEL PROYECTO

Título

Herramientas jurídicas para la protección de los datos personales en Colombia: Análisis del grado de protección jurídica del Habeas Data.

Planteamiento del problema

La recolección y tratamiento de la información realizada por las empresas en el siglo XX no tenía una importancia económica, pero con la entrada progresiva de los medios tecnológicos, bases de datos virtuales y el intercambio transfronterizo de datos que permitió la red de internet, la información se vuelve útil para la creación de estrategias y acciones en las empresas y entidades. La recolección frecuente de datos personales cambia las relaciones con las personas que los facilitan, objeto del tratamiento para acceder a los servicios que lo exigen.

Esta actividad fue regulada primigeniamente a través de la voluntad particular de cada empresa, quienes establecían unas directrices sobre tratamiento de privacidad, modelo prevalente en Estados Unidos. Posteriormente en la Unión Europea se acogió la postura estatal de regulación, que consiste en su incorporación como derecho fundamental dentro de las constituciones de los países europeos y en la expedición de leyes que otorgaban funciones a las autoridades administrativas y competencias a las judiciales.

América Latina no fue ajena a esta tendencia, siendo Argentina y Brasil los primeros en incorporar leyes al respecto. Durante la década de los 90 otros países incorporaron como derecho fundamental el Habeas Data y garantizaron su efectividad por medio del recurso de

amparo como instrumento jurídico. Colombia adoptó esta tendencia a través de la incorporación en el artículo 15 de la Constitución de 1991, siendo desarrollado jurisprudencialmente por la Corte Constitucional colombiana en múltiples sentencias y por el Congreso de la República tardíamente mediante las leyes 1266 de 2008 y 1581 de 2012.

Existe la preocupación a nivel internacional, sobre el cumplimiento de los estándares adecuados para proteger los derechos del Habeas Data de la regulación normativa existente en Colombia, porque la vía procesal del recurso de amparo colombiano es la herramienta más frecuente con la que acuden las personas que se les vulnera el derecho al habeas data.

Los análisis realizados sobre cada uno de los mecanismos normativos para la protección de datos personales, así como la posterior descripción de las características, derechos y elementos estructurales permitirán concluir el grado de protección jurídica de cada una de ellas para encauzar los casos específicos de vulneración del Habeas Data a la más adecuada.

Permitir la continuidad de este desconocimiento, de los mecanismos para proteger los derechos al habeas data, generaría una sobrecarga en los mecanismos de la Autoridad Nacional de Protección de Datos (la Superintendencia Industria y Comercio) o en el recurso de amparo (llamado en Colombia Acción de tutela) de casos de vulneración, cuya resoluciones más pertinente por los otros mecanismos porque pueden garantizar una protección más provechosa para el titular afectado en su interés jurídico, por el indebido tratamiento, en su intimidad, buen nombre u otros derechos.

Para contrarrestar esta situación se propone analizar el grado de protección jurídica del Habeas Dataa través de las Herramientas jurídicas para la protección de los datos personales en Colombia.

Formulación del problema

¿Cuál es el grado de protección jurídica adecuada que ofrecen las herramientas jurídicas para la protección de datos personales en Colombia?

Sistematización del problema

¿Cuáles son las características estructurales de las herramientas jurídicas para la protección de datos personales vigentes en Colombia?

¿Qué derechos del Habeas Data protegen las herramientas jurídicas en Colombia?

¿Cuál es el grado de protección jurídica que ofrecen, ante una posible vulneración de los derechos al Habeas Data en Colombia, frente a los modelos europeo y norteamericano de protección de datos?

Justificación

Los países a raíz de la declaración del derecho fundamental a la privacidad y al debido tratamiento de los datos, se han preocupado por legislar acerca de los procedimientos y reglas adecuados para evitar su afectación en los titulares del derecho. Las nuevas tecnologías han permitido flexibilidad en el flujo de la información a través de los dispositivos tecnológicos que portan las personas con diversas aplicaciones, las cuales generan un intercambio constante e internacional de datos con servidores de todo el mundo.

La preocupación sobre la posible afectación en los derechos de la persona al Habeas Data, surge sobre la incertidumbre de que las empresas o entidades traten la información adecuadamente, otorgando mecanismos de control a las personas en la salvaguarda de sus derechos. En Colombia a pesar de tener una ley sobre la temática, las personas desconocen la cobertura de los mecanismos existentes y han recurrido a la acción de tutela como mecanismo principal.

Este trabajo pretende abordar a nivel nacional, con el análisis jurídico, la temática de los mecanismos de protección del habeas data, desde que se expidiera la ley 1581 de 2012, siendo necesario este abordaje para facilitar su comprensión entre las personas.

Para las entidades responsables y/o encargadas del tratamiento de datos personales, a nivel regional, como las entidades públicas o a nivel institucional, como la Universidad Libre, entre otros, es importante y oportuno este proyecto porque les ofrece un conocimiento claro y preciso del desarrollo sistemático del marco legal, a partir del cual tendrán que adaptar o crear políticas de tratamiento de información y procedimientos para resolver solicitudes, sin que estos vulneren el Habeas Data.

Por todo lo anterior la importancia social de este proyecto de investigación es la difusión del análisis de los instrumentos legales existentes para que las personas puedan evitar un uso inadecuado o no autorizado de sus datos personales, por las vías procesales o administrativas, creadas para la garantía de los derechos fundamentales a la privacidad, al habeas data y al buen nombre.

Objetivos

Objetivo general

Analizar el grado de protección del derecho al Habeas Data por las herramientas jurídicas para la protección de datos personales en Colombia utilizando los estándares de protección de datos personales que estableció la Comunidad Europea de Naciones y los Estados Unidos de América

Objetivos específicos

Describir las herramientas jurídicas para la protección de datos personales en Colombia vigentes en la ley.

Diferenciar los derechos del Habeas Data que garantizan los mecanismos para la protección de datos personales en Colombia.

Comparar el grado de protección jurídica que ofrecen las herramientas vigentes en el sistema normativo colombiano, ante posibles casos de vulneración del Habeas Data en Colombia, frente a los modelos europeo y norteamericano de protección de datos personales.

MARCO DE REFERENCIA

Antecedentes

El Trabajo de Grado “ Sanciones por parte de la Superintendencia de Industria y Comercio por el Cambio de la Finalidad en el uso de los datos personales en Colombia, Período 2013-2014” realizado por Angelica María Paez Escobar y José Daniel Vera Ayala(2015:7-8) que estudió las sanciones que impuso la Superintendencia de Industria y Comercio de Colombia durante el período 2013-214 para identificar la aplicación de las facultades que ejerce como Autoridad Nacional de Protección de Datos Personales y conocer los resultados de esas sanciones.

El Trabajo de Grado, “Habeas data y protección a los datos personales”, realizado por Milena Parra Rincón y Yineth Johana Savogal (2008) centra su análisis en el habeas data y la responsabilidad civil generada por los daños que causa el responsable o encargado de tratamiento de datos personales al titular del dato personal.

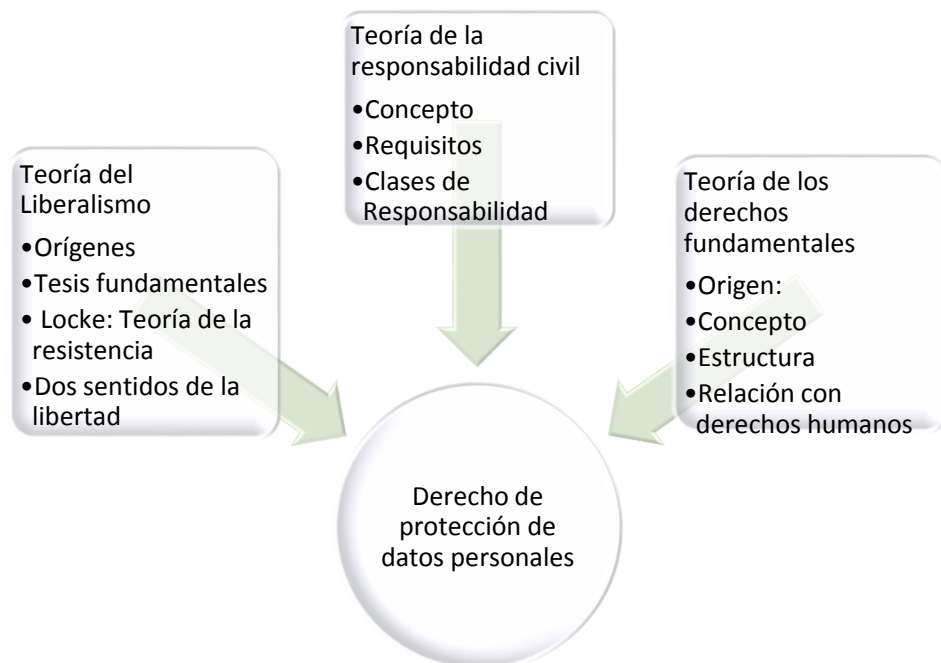
El Trabajo de Grado, “La protección de la información y los datos como delito informático en Colombia: sanciones penales” (2009 o 2010), cuyo objeto de estudio es la Ley 1273 de 2009, que crea tipos penales para el nuevo bien jurídico de la protección de la información y los datos, con un análisis integral a las normas, sus desventajas y ventajas, a los tipos penales y finalizando con una entrevista a los gerentes de empresas informáticas de Cúcuta.

El Trabajo de Grado. “Implicaciones a partir de la aplicación de la nueva legislación respecto al Habeas Data” (2008) cuyo principal aporte es el estudio de la efectividad de los mecanismos fijados por la ley 1266 de 2008 en la protección del titular del dato personal.

Bases teóricas

Investigación jurídica

Las teorías que fundamentan la presente investigación jurídica se nutren de cinco lugares del conocimiento humano como son la filosofía política, filosofía del derecho, el derecho civil, el derecho constitucional y los derechos humanos. Dichas teorías son expuestas a continuación en el orden de aparición histórica: la teoría del liberalismo político, la teoría de los derechos fundamentales, la teoría de los derechos humanos y la teoría de la responsabilidad civil.



Fuente: Camilo Puello. Enero 2016

Teoría del liberalismo

La teoría liberalismo político surge con las propuestas teóricas de John Locke y Jean Jacques Rousseau, que reflexionan sobre la idea de un derecho a gobernarse por sí mismo (Locke, 2006:10) y otro derecho a constituir un gobierno que regule los intereses jurídicos de todos.

La teoría liberal de John Locke, propuesta en su “Segundo Tratado sobre el Gobierno Civil”(2006), es la base inicial de la preocupación del derecho por el ser humano de protegerle sus bienes básicos por sí mismo o instrumentos externos(en el caso que lo plantea significa la vuelta al estado de guerra) ; el presupuesto fundamental es la necesidad de conservar la libertad del estado natural, inclusive cuando se asocian para superar el estado de guerra y darse una autoridad común que ordene paz, porque se ve expuesta a su vulneración por el arbitrio de otro en defensa excesiva o por agresión inminente (Cortés, 2010:103), lo cual merma las potencialidades y aspiraciones de vida.

Junto a la autoridad común propone el derecho a la propiedad, que define como el respeto a las condiciones de posesión de unos bienes materiales y morales, en estos últimos destaca la paz, la vida, la libertad y la inviolabilidad corporal (Locke, 1991:27 citado por Cortés, 2010). Los bienes materiales se vuelven propios por efecto de transformarlos del estado natural y los bienes morales a los que alude son su propio cuerpo y sus capacidades, propias por ser libre.² Para proteger todos estos bienes que han logrado se acuerda un poder político superior pero limitado a conservar su libertad, porque “(...) es tan necesaria y se halla indisolublemente ligada a la preservación del hombre que no cabe renunciar a aquella sin perder la vida y la salvaguarda a un tiempo”(Locke, 1991:23)

De esta manera cuando el gobierno va contra el contrato que lo originó es posible rebelarse las personas(Locke, 1991:202), proponiendo una teoría de la resistencia, que implica una vuelta al estado de guerra y lucha por recuperar lo perdido.Esta idea se tomará durante el desarrollo de la investigación como uno de los soportes para justificar la separación del *derecho al debido tratamiento de los datos personales* del *derecho a la intimidad*.

La libertad en sentido Lockeano es entendida como un estado que permite a “(...) cada uno ordene sus acciones y disponga de posesiones y personas como juzgue oportuno, dentro de los límites de la ley de la naturaleza, sin pedir permiso ni depender de la voluntad de

² Hasta este punto el hombre es igual a todos, pero Locke afirma que la invención de la moneda genera una desigualdad inherente porque permite (i) la acumulación de bienes sin degradación al crearse un equivalente cambiario (ii) satisfacción de necesidades superiores a las básicas (iii) un excedente que permite comprar fuerza de trabajo. (CORTÉS, 2010:115)

ningún otro hombre” (Locke, 2006:10). Esa ley de la naturaleza establece los límites “(...) que gobierna y que obliga a todos; y la razón, que es esa ley, enseña a toda la humanidad que quiera consultarla que siendo todos los hombres iguales e independientes, ninguno debe dañar al otro (...)” (Locke, 2006:12,60)

Por otro lado, la teoría de la resistencia es planteada como una manera de conseguir que sea observada la ley natural porque de lo contrario sería inútil que existiera, (Locke, 2006:13), es el poder para ejecutar la ley natural. Así lo dice en varios apartes Locke (2006):

“Pues como todo poder que se concede con el encargo de cumplir un fin determinado ha de limitarse a la consecución de ese fin, siempre que el fin en cuestión sea manifiestamente olvidado o antagonizado resultará necesario retirar la confianza que se había puesto en quienes tenían la misión de cumplirlo; y así el poder volverá a manos de aquellos que lo concedieron, los cuales podrán disponer de él como les parezca más conveniente para su protección y seguridad” (Locke, 2006: 147 y ss.)

(...)

“Por lo tanto, siempre que el poder legislativo viole esta ley fundamental de la sociedad, y ya sea por ambición, por miedo, por insensatez o por corrupción, trate de acumular excesivo poder o de depositarlo en manos de cualquier otro, es decir, un poder sobre las vidas, libertades y los bienes de un pueblo, estará traicionando su misión; y por ello mismo, estará trocando el poder que el pueblo puso en sus manos por otro con fines distintos”(Locke,2006:212)

Es pues un derecho a oponerse cuando se ejercitan acciones contrarias a la misión u objetivo legal permitido. (Locke, 2006:218 y ss.)

Desde la teoría liberal de Locke se tomarán las nociones de libertad y resistencia conforme a los planteamientos desarrollados previamente. A partir de estos conceptos fundamentales surgen *las teorías del estado derecho, de la personalidad jurídica y de los derechos humanos*, fundamentalmente motivadas razones políticas y razones económicas que inciden en el cambio en la mentalidad de los pensadores (Peces-Barba, 1986:231-234)

Teoría de los derechos fundamentales

Para entender mejor el modelo europeo de protección de datos personales, se aborda no solo la *teoría de los derechos fundamentales* sino también el apoyo que le da para sustentarle la *teoría del estado de derecho*. “Con frecuencia existe una estrecha conexión entre derechos humanos y organización del estado, y difícilmente se duda de ello” (Alexy, 2000:21)

En este sentido la perspectiva teórica a adoptar corresponde a su formulación para el caso de los derechos fundamentales de la teoría propuesta por Robert Alexy en su libro *Teoría de los derechos fundamentales*, Ernst-Wolfgang Böckenförde en su libro *Escritos sobre derechos fundamentales* y Antonio Pérez-Luño en su libro *Los derechos fundamentales*; para la teoría del estado de derecho se acogen los planteamientos de Ernst-Wolfgang Böckenförde en su artículo “Origen y cambio del concepto de estado de derecho” que se puede encontrar en su libro *Estudios sobre el estado de derecho y la democracia*.

.

Teoría del Estado

El concepto de *Estado de derecho*, que se ha extendido a múltiples idiomas, surge como desarrollo del liberalismo en tierra alemana, “es el estado de derecho racional, esto es, el estado que realiza los principios de la razón en y para la vida en común de los hombres, tal y como estaban formulados en la tradición de la teoría del derecho racional” (Böckenförde, 2000:19).

El concepto proviene en su versión simple de Kant, quien lo formula como “la unión de hombres bajo leyes”(Kant, 1797: par.45, 43 y especialmente 52 cit. por Böckenforde, 2000: p.), luego se incluirá el propósito esta unión en el interés común de los ciudadanos, retomando un poco el planteamiento lockeano de legitimidad del estado.

Otto Mayer (citado por Böckenforde, 2000:26) incluye la característica de orden, buena administración y derecho constitucional como elementos que permiten al ciudadano la garantía de sus derechos frente al ejecutivo.

Otto Bähr y Otto von Gierke (citado por Böckenforde, 2000:28) resaltan el elemento de derecho porque toda la creación, ejercicio y relación de los órganos estatales se ejerce a partir del derecho fijado en la Constitución, quien controla su cumplimiento por vía de los jueces de la nueva jurisdicción constitucional.

Finalmente Anschütz desarrolla el planteamiento de la fuente de la ley, abandonando la teoría de su origen racional al resaltar la labor del legislador y la garantía judicial como tareas imprescindibles para que se mantenga el imperio de la ley. (cit. por Böckenforde, 2000:29). Aquí se llega al máximo culmen de la teoría formal del Estado de Derecho o Estado de Derecho Liberal y comienzan a generarse los problemas de la cuestión social. Esta problemática se presentó por solicitudes al Estado de intervenir para el logro de mayor igualdad material, protección al trabajador y acceso a oportunidades, para que los tres pilares básicos del estado (igualdad, derecho a la propiedad y libertad) se materialicen para muchos.

El Estado social de derecho como modelo de estado alterno surge para contrarrestar estos últimos problemas y ofrecer la igualdad material y social a través de la redistribución de bienes. (Bockenforde, 2000:33)

La teoría del estado de derecho, en un sentido moderno, acude a su actualización con la inclusión de la palabra “*social*” para indicar que se está ante un estado material de derecho que no solo tiene la función de defensa o garantía de los derechos fundamentales de las personas sino también lograr la efectividad progresiva de los principios, valores y derechos fundamentales para la sociedad que los ha elegido como parte de su Constitución. El concepto de estado social de derecho se desintegra en los siguientes aspectos:

1. La renuncia a un fin metafísico de la existencia del estado y su centro es el individuo libre, autónomo, igual y racional. Se puede apreciar cuando dice Böckenforde que:

”El concepto del Estado de derecho incluye una tendencia hacia la libertad (...). La libertad política de los ciudadanos, su participación activa en la vida del estado vale

como culminación y garantía de la libertad civil, pero encuentra su límite allí donde no llega la protección de la libertad civil, (...) donde deja de dar preferencia a la razón y se inclina a favor de los meros deseos o intereses” (Böckenforde, 2000:22)

2. El estado de derecho es la referencia a la garantía de la libertad personal, que protege al individuo y la limitación del poder del estado es una garantía para el desarrollo individual (Böckenforde, 2000:44). Es la conciencia de responder a través de mecanismos jurisdiccionales frente a las injerencias externas de otros individuos o del Estado mismo. “La sumisión de la administración al control de los tribunales aparece así como la perfección de la construcción asociativa del Estado y como garantía del imperio del Derecho en el Estado.” (Böckenforde, 2000:28)

3. El estado debe actuar bajo los principios racionales: libertades civiles, igualdad jurídica, respeto a la propiedad, imparcialidad e independencia judicial, participación del pueblo y la división de poderes. Se vincula a estos principios mediante la ley, que obliga jurídicamente a la acción y al límite de sus actos. (Böckenforde, 2000:27)

4. La Constitución ofrece planteamiento marco de los tres postulados básicos (libertad, igualdad jurídica y derecho a la propiedad) así como de los derechos sociales. Sin embargo el ámbito para decidir las contradicciones sociales y propender por la igualdad real debe ser en la ley que expide el Parlamento y la administración (Böckenforde, 2000:37)

5. Flexibilización de los tres postulados básicos del Estado de derecho. Por ejemplo del principio de igualdad ante la ley en algunos casos con el fin de estimular la igualdad real. Del derecho a la propiedad cuando el estado dispone para lograr sus fines sociales de una mayor carga fiscal a los individuos.

6. Tensión entre los postulados básicos de la libertad, la igualdad jurídica y la propiedad en el concepto originario del Estado de derecho y los postulados axiológicos. En efecto porque no hay un sistema racionalmente fundado para resolver esos valores y

que indique de forma satisfactoria la conformidad de la elección con el desarrollo del valor, afectando la libertad y la autonomía individuales(Bockenforde,2000:42)

Teoría de los derechos fundamentales

Sin la existencia del estado de derecho no valdrían los derechos fundamentales, porque estos implican la existencia de un conjunto de posiciones e interés del sujeto que son reconocidas y protegidas por el Estado (Pèrez-Luño, Antonio, 2004:19)

La teoría de los derechos fundamentales surgió para estudiar la manera como se relacionan ciertas libertades de acción o derechos ciudadanos, reconocidos positivamente, con el poder estatal y su actividad pública, sobre la base de la jurisprudencia de los tribunales constitucionales de cada país. Se deduce el objeto de estudio de los derechos fundamentales de acuerdo a lo expresado por Pérez Luño (2004:20):“Los derechos se presentan en la normativa constitucional como un conjunto de valores objetivos básicos y al propio tiempo como el marco de protección de las situaciones jurídicas subjetivas” y Robert Alexy (1993:23) acerca de lo que es la teoría de los derechos fundamentales:

“Lo que hoy son derechos fundamentales es definido principalmente sobre la base de la jurisprudencia del Tribunal Constitucional Federal. La ciencia de los derechos fundamentales – no obstante la controversia acerca de la fuerza vinculante de las decisiones del Tribunal Constitucional - se ha convertido, en una apreciable medida, en una ciencia de la jurisprudencia constitucional.”

Robert Alexy (1993:34) justifica una teoría general de los derechos fundamentales centrada en el análisis de los derechos fundamentales de la constitución alemana bajo la óptica normativa, empírica y analítica.

Robert Alexy(1993:27 y ss.) realiza un profundo análisis sobre la definición de norma de derecho fundamental y su estructura. Este trabajo de investigación resume los elementos en:

1. Es un enunciado normativo-semántico
2. Se encuentran en la constitución (criterio formal) para conferir derechos subjetivos(criterio material) y estar dentro del mismo fundamento del estado (criterio material); “(...) son sólo aquellas que son expresadas directamente por enunciados de la LF(disposiciones de derecho fundamental)”(Alexy,1993:66)
3. Algunas son integradas o concretizadas para casos específicos, por ello se les llama normas adscriptas, Otras, son estatuidas directamente del texto constitucional.
4. Tienen una estructura que las define como derechos a algo, libertades o competencias.

La teoría de Robert Alexy es de utilidad para esta investigación en la formulación práctica del derecho de libertad y el método para resolver conflictos de intereses que poseen el mismo rango a nivel constitucional cuando se entran a analizar la jurisprudencia constitucional. Porque es el método escogido al momento de analizar el grado de protección jurídica de los mecanismos y la elección de aquel que aumenta la esfera de efectividad del derecho general al habeas data.

El análisis que realiza respecto a la estructura de las normas de derecho fundamental, definiéndolas como enunciados normativos(Alexy,2007:47 y ss.) que establecen posiciones jurídicas que reconocen algo frente al otro, entendido este como el Estado o las personas jurídicas o naturales. Las posiciones que concibe Alexy(P.163) pueden ser clasificadas en derechos a algo, libertades y competencias. Es importante esta clasificación para el análisis estructural del derecho fundamental que es el habeas data, comprender analíticamente la evolución jurisprudencial de la Corte Constitucional colombiana y conocer tanto los derechos como el nivel de protección que tienen los mecanismos vigentes en el ordenamiento jurídico.

El concepto de norma fundamental, bajo la perspectiva que Alexy propone, tiene una estructura compuesta de: principios y reglas (Alexy, 2007:63) que se manifiesta de dos maneras posibles en la Constitución: como *principio* cuando “(...) ordena que algo sea realizado en la mayor medida posible, dentro de las posibilidades jurídicas y reales existentes (...)” (Alexy, 2007:67), es decir, que hay posibilidad de “jugar” y argumentar, en su iusfundamentación, el grado de cumplimiento según los casos y enfrentamientos que ocurran; y como regla cuando no da otra posibilidad más que actuar conforme a ella o no actuar conforme a ella (Alexy, 2007:68).

Teoría de los derechos humanos

La libertad es el germen de todos los derechos humanos, incluso de los otros principios hermanos que son la igualdad y la dignidad (Alexy, 2007:311), porque su limitación puede conseguirse a través de múltiples maneras, por ejemplo obstaculizar la acción para conseguir las profundas aspiraciones de cada persona (dignidad), “(...) ser restringido arbitrariamente en la libertad, es algo que contradice la dignidad humana (...)” (Alexy, 2007:314) e impedir, sin argumento justificado, el acceso a las oportunidades que permite materializar las aspiraciones perseguidas (igualdad).

Esta afirmación se deduce de algunas definiciones dadas por los doctrinantes de derechos humanos: Ernesto Rey Cantor y María Carolina Rodríguez (2005:251) afirman que “(...) son aquellos que todos los seres humanos tienen para vivir dignamente como hermanos fraternales”, el profesor German Bidart (1989:234) lo ubica en el plano de suprapositividad donde se “definen exigencias acordes con la dignidad de la persona y los valores (...)”, Eusebio Fernández (cit. por Bidart, 1989:234) lo define de manera positiva, como lo que “(...) consideramos deseable, importante y bueno para el desarrollo de la vida humana (...)” y por último el profesor Antonio Pérez Luño (Cit. por Bidart, 1989:233) nos confirma los argumentos al decir que los derechos humanos son “(...) conjunto de facultades e instituciones que en cada momento histórico, concretan las exigencias de la dignidad, la libertad y la igualdad humanas (...)”

La teoría de los derechos humanos se encarga de estudiar el conjunto de derechos subjetivos naturales que le pertenecen al hombre por hacer parte de su misma naturaleza en un momento determinado. Ahora dentro de esta rama pueden hacerse estudios sobre el origen e impacto normativo de los derechos humanos en contextos temporalmente determinados, bajo esta afirmación se convierten en objetos de una historia de los derechos humanos, “(...)la más pura fundamentación exclusivamente racional, es necesariamente también fundamentación histórica (...) que intenta descubrir las causas de aparición de los derechos humanos y las razones que tuvieron los hombres desde el siglo XVI para pensarlos e impulsarlos en la realidad” (Peces-Barba,:268) ; es necesario que al estudiar los derechos humanos no se olvide el contexto histórico porque permite realizar el análisis específico de ellos.

Los doctrinantes de derechos humanos están de acuerdo en el postulado de las *generaciones de los derechos humanos*. Este concepto se justifica para explicar la aparición sucesiva de derechos, agrupados por momentos impactantes de la historia moderna y contemporánea (Rey Cantor & Rodríguez, 2005:23), porque los derechos humanos surgen por necesidades de una sociedad y momento específico. (Pérez, 2006:34)(Peces-Barba, 1988:269)

Los derechos humanos surgen como defensa ante el avance del Estado Absoluto, intentando modificar su naturaleza para limitar sus competencias (en el sentido de Alexy, 2007:) y ante la aspiración de permitir que todos se liberasen de las ataduras del viejo feudalismo bajo los postulados de igualdad y libertad. Ambos permiten el ejercicio de una fuerza de oposición cuando no se respeten los derechos y exigir que se garanticen frente a cualquier intervención (Bobbio, 1989:11 cit. por Rey Cantor&Rodríguez, 2005:31); los derechos humanos se formularon originariamente de esta manera porque la concepción inicial fue iusnaturalista, lo cual significó que eran suprapositivos e imbricados profundamente en la naturaleza humana (Peces-Barba, 1988:275). Posteriormente pasaron por una etapa de positivización para intentar darles mayor eficacia jurídica. (Peces-Barba, 1986: 242)

Los derechos humanos son el desarrollo de los límites de la libertad de las personas cuando se convive en sociedad. “El fundamento de los derechos humanos es la realización de

esa función de la libertad social-política y jurídica como cauce del desarrollo de la dignidad humana que supone el dinamismo de la libertad de elección a la libertad moral” (Peces-Barba, 1988:272).

Por otro lado los derechos fundamentales también tienen su origen en el mismo principio de la libertad, que debe protegerse frente a interferencias estatales y privadas. Se menciona partes de lo que comenta el profesor Antonio Pérez Luño sobre la conversión en normas de los principios de derecho natural, pensados por los filósofos a raíz del cambio histórico devenido con el siglo de las luces, entre esos el de la libertad: “La nueva expresión [derechos del hombre] al igual la de “derechos fundamentales”, forjada también en este período [mitad del siglo XVIII], revela la aspiración del iusnaturalismo iluminista por constitucionalizar, o sea, por convertirse en derecho positivo, en preceptos del máximo rango normativo, los derechos naturales” (Perez,2004:33)

Como ambos tipos de derechos subjetivos tienen un núcleo común, la libertad (Pérez,2004:29), es adecuado afirmar que los derechos humanos pueden ser entendidos bajo la misma definición de Alexy, como enunciados deónticos, que establecen como correlación un deber de hacer u omitir algo, situación que no enaltece las obligaciones, porque la teoría de los derechos humanos habla de la preeminencia del sujeto para exigir su derecho frente a los demás que se encuentran obligados, es decir, que mi derecho como sujeto preexiste a los deberes que genera cada individuo, pero descontando el hecho de que se encuentran fijados en tratados de orden internacional y no limitados a la Carta Magna.

Teoría de la responsabilidad civil

Las consecuencias de la vulneración del Habeas Data implican dos posibles reacciones jurídicas: i) la investigación administrativa o penal para sancionar la conducta del administrador de la base de datos (encargado o responsable del tratamiento) y ii) el reconocimiento al titular del dato vulnerado de un derecho a la reparación. Estamos en el

primer caso ante el derecho sancionatorio, en sentido lato, y en el segundo caso frente a una responsabilidad civil, porque “(...) engloba todos los comportamientos ilícitos que por generar daño a terceros hacen recaer en cabeza de quien lo causó, la obligación de indemnizar” (Tamayo, 2007:8) como bien lo define Tamayo (2007:8)

En cuanto a la teoría de la responsabilidad civil, se apoya la investigación en lo propuesto por Adriano de Cupis en su libro *El Daño, Teoría general de la responsabilidad civil*, Arturo Alessandri en su libro *Derecho de la responsabilidad extracontractual en el derecho civil chileno* y Javier Tamayo Jaramillo en su libro *Tratado de la Responsabilidad Civil*.

Concepto

Toda conducta realizada por el hombre generará efectos jurídicos, bajo la teoría de los hechos jurídicos, algunos serán queridos y conformes a la ley (Tamayo, 2007:5), otros no reunirán estos dos aspectos, como el incumplimiento de la obligación o serán realizados bajo negligencia o culpa. Los primeros serán los actos lícitos, que son aquellos actos tendientes a establecer obligaciones jurídicas entre dos personas de manera unilateral o bilateral dentro del ordenamiento jurídico; los segundos, en su ejecución serán actos ilícitos porque transgreden la norma y afectan intereses públicos o privados.

Los actos ilícitos o transgresores de la norma pueden generar reacciones del ordenamiento jurídico como devenir en nulos(o inexistentes o ineficaces según el caso) o sancionar con pena al que lo realizó (porque atentó contra el bien jurídico protegido por la ley penal) o con reparación del perjuicio, que esa transgresión generó, a la persona que lo sufrió. El profesor Tamayo Jaramillo hace una muy buena distinción de los hechos ilícitos al clasificarlos en faltas penales y faltas civiles, siendo estos últimos aquellos hechos ilícitos y que causen un daño y a partir de los que se desprende la responsabilidad civil, que es la obligación de una reparación. Al respecto Tamayo (2007:7) reafirma lo anterior al decir que:

“Como se ve, el hecho ilícito consiste siempre en el incumplimiento de obligaciones contractuales, cuasicontractuales, legales o simplemente en el incumplimiento del deber general de prudencia. De allí que podamos afirmar que la responsabilidad civil encuentra su fundamento jurídico en los hechos ilícitos (...)”

El objeto de esa reparación es la generación de un equilibrio patrimonial entre el afectado y quien cometió el hecho ilícito. Por lo anterior se puede afirmar que el objeto de estudio de la responsabilidad civil es la manera como puede equilibrar la reparación el patrimonio afectado por la acción de otra persona que obtuvo con ello un beneficio. En el mismo sentido opina Alessandri (1943:28) al decir que “(...) es precisamente *reparar ese daño*, dejar indemne el patrimonio que lo ha sufrido”

Requisitos

Los actos ilícitos cometidos por una persona a la cual se le adjudica la responsabilidad civil requieren de tres elementos para que exista responsabilidad civil: conducta de esa persona u otra a su cargo, daño a otro(Alessandri, 1943:28), necesidad de nexo causal entre el hecho dañoso y la conducta.

El sufrimiento, afectación o destrucción del interés jurídico se denomina daño, definido como “la alteración negativa de un estado de cosas existentes” (Henao ,1998:84), cuyas consecuencias implicaría una serie de acontecimientos desfavorables para la persona desde el plano económico o moral, lo que se llama perjuicio se compone “(...) el conjunto de elementos que aparecen como las diversas consecuencias que se derivan del daño para la víctima del mismo”(Bénoit, “Essai sur les conditions de la responsabilité en droit public et privé”, citado por Henao,1998:77)

El objeto del daño es la afectación del interés humano tutelado jurídicamente, entendido como lo manifiesta De Cupis (1978:111) de “necesidad, experimentada por uno o varios sujetos determinados, que venga satisfecha mediante un bien”. Se habla de interés humano en

general, pero se tomará en cuenta aquel interés de un sujeto o sujetos específicos e individuales y con potencial valor patrimonial o carente de él, pero cuyo rasgo común es ser de interés para el ordenamiento jurídico.

Clases de Responsabilidad

Ahora en cuanto a quien comete el daño, tomaremos el criterio según el grado de control que puede tener la persona en la materialización del daño, según esta la teoría de la responsabilidad civil distingue en directa e indirecta. La primera cuando se responde por el hecho propio y la segunda cuando el daño causado por el hecho de una tercera persona o bien del daño originado en el hecho de las cosas (aquel daño cuya génesis se encuentra en la omisión inicial de un acto humano) o bien como dice De Cupis (1978:130) “(...) participación del ser humano en el desenvolvimiento del proceso dañoso derivado de las cosas”.

La responsabilidad directa puede ser contractual o extracontractual, mientras que la indirecta casi siempre será extracontractual.

La *responsabilidad contractual* se origina en la violación del artículo 1602 del Código Civil colombiano que afirma la obligatoriedad del cumplimiento del acuerdo o contrato entre las partes, por ello cuando se incumple, se genera una frustración a la expectativa legítima de cumplimiento provocando una alteración del derecho ya adquirido preexistente que se ve “borrado”, ocurre lo que menciona Alessandri (1943:42); “(...)la obligación de indemnizar al acreedor el perjuicio que le causa el incumplimiento del contrato o su cumplimiento tardío.”

La *responsabilidad extracontractual* (delictual o cuasidelictual) proviene de un hecho ilícito civil producido por una persona, con intención o no, que lesiona a otra; en este tipo de responsabilidad no existe obligación preexistente y se basa en el principio genérico de que toda persona responderá por los daños causados. Esta clase de responsabilidad se fija el artículo 2343 del Código Civil colombiano. Alessandri (1943:43) lo resume en que el daño es el mismo generador de la obligación de reparar. Este tipo de responsabilidad cuando se funda

en el dolo o culpa de la persona es subjetiva; cuando se funda en el riesgo latente de la actividad, es objetiva.

Surgimiento de la responsabilidad civil por indebido tratamiento de datos personales

La teoría de la responsabilidad civil es un soporte teórico pertinente para esta investigación porque un indebido tratamiento de datos personales producirá diversas afectaciones, dependiendo de si afectan aspectos patrimoniales o no patrimoniales de la persona. Además la acción de responsabilidad civil es uno de los mecanismos identificados y sus variantes dependerá de la fuente que la genere: incumplimiento de un contrato o de la norma más general de sanción a hechos ilícitos y del tipo de agresor causante del hecho productor del daño, una persona de derecho privado o una persona de derecho público.

De Cupis (1978:153) explica las diferencias entre daño contractual frente al extracontractual:

“Ciertamente que el vínculo obligatorio contractual mediante la integración que hemos visto, puede extenderse más allá de cuanto han previsto las partes del contrato, pero no puede llegar a comprender lo que es totalmente extraño a la índole de la prestación convenida”

El daño se presenta como un puente entre el hecho generador de este y la norma jurídica y es importante para determinar la intensidad de la afectación de la norma jurídica (De Cupis, 1978:83 y ss.)

Así las cosas, frente al indebido tratamiento de datos personales, el interés jurídico que se protege es la intimidad, el buen nombre y la honra. Según la forma en que sea “sacrificado” el sujeto pasivo, se afirma que el interés del sujeto es el cumplimiento de los lineamientos de la política de privacidad fijada y que está no produzca una afectación per se, esto es en cumplimiento de una obligación contractual; habrá daño extracontractual cuando la recolección o tratamiento se realizó sin que haya obtenido la autorización para realizar el

tratamiento con una finalidad, que es el generador del vínculo jurídico, y se produzca como consecuencia de esto un daño.

Habeas Data - protección de datos

El surgimiento del derecho a la protección de datos personales se deriva del principio general de la libertad de la persona y el reconocimiento de su personalidad jurídica, producto del individualismo racional de los siglos XVIII y XIX. Este principio se manifestó en la proclama imponer pocas limitaciones jurídicas a los individuos por la ley (Del Vecchio, 1971, p.86) y conllevó al desarrollo primigenio del derecho a la intimidad o privacidad, consistente en una abstención del Estado a molestar a las personas lo menos posible, regulándose las excepciones habilitantes por la ley.

Para el derecho a la intimidad, de la mitad del siglo XX en adelante, surge la amenaza potencial de las tecnologías automatizadas de tratamientos de datos personales (Remolina-Angarita, 1994, P.192)(Pérez Luño,2008:32) que acumulan información y generan una nueva clase de poder sobre las personas: el poder informático.

Al final del siglo XX el poder informático aumenta su influencia a costa de la efectividad relativa de las facultades otorgadas a los sujetos (Remolina Angarita, 2013:2) motivado por conseguir el uso eficiente y analítico de la información a raíz de las invenciones de nuevas tecnologías de la información y la comunicación; la situación en el siglo pasado planteó otra amenaza al bien jurídico de la información personal: un indebido tratamiento de información.

La preocupación ante el avance de ese poder informático, es perder la libertad de decisión y elección en la administración de lo que otros saben o conocieron de nosotros en un momento determinado con o sin nuestro permiso. Para protegerse del poder informático se desprende de la libertad de la persona y su correlativa obligación de no ser molestado nuevos derechos: en el espacio europeo, el derecho a la autodeterminación informativa(Suárez Espino,2008:9,52 y ss.), una nueva facultad jurídica al sujeto de controlar e informarse sobre

la manera en que se usan los datos que se almacenan por parte de otras personas naturales o jurídicas, reduciendo su enorme poder informático; y en el lado norteamericano la tutela de los datos de las personas mediante una especialización del derecho a la intimidad, que llaman *privacy*.

El tratamiento adecuado de la información personal debe reconocerse como derecho fundamental por cuatro razones según Saarenpää (2003): “las exigencias de la democracia, la sociedad red, la búsqueda de la eficiencia y el complejo curso vital de la información”. Las condiciones del procesamiento de datos le dificultan a la persona el control del uso de sus datos y la calidad de la información. Este nuevo derecho surge para vincular las organizaciones tratantes o recolectoras de información personal a un cambio en las políticas de tratamiento de la información según los estándares y principios formulados alrededor del mundo.

Los elementos teóricos principales que conforman el modelo de protección del derecho al habeas data son: los sujetos (titular del derecho, responsable del tratamiento, encargado del tratamiento), un objeto tutelado jurídicamente (dato personal, bases de datos personales), hechos con consecuencias jurídicas (el tratamiento, la autorización) y los procesos, acciones procesales y actos jurídicos que enmarcan dicha relación y fijan los parámetros de tratamiento que configuran unos derechos, deberes y obligaciones de los sujetos.

El *dato personal* es cualquier preferencia, conducta o cualidad que se refiere a una persona, pueden hacer referencia a: familia, transacciones financieras, salud, solvencia económica, creencias religiosas, procesos y condenas criminales, origen racial y étnico, títulos y grados académicos y preferencias personales e internas (Remolina, 2010a:492). Cuando se encuentran reunidos en un solo lugar información de muchas personas se denominarán *bases datos personales*.

Autorización es toda manifestación, expresa o concluyente de la voluntad, realizada por la persona que es titular del dato, para permitir el tratamiento respectivo de su dato o datos personales.

El *tratamiento de datos personales* se presenta cuando hay recolección, registro, organización, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, destrucción y difusión. La forma en que se realizan estas operaciones y los fines perseguidos con los datos han generado los modelos europeo y norteamericano de protección de datos personales.

Los *sujetos* que participan en el tratamiento de datos son el titular del dato personal, quien es el dueño de la información que solicita otra persona jurídica o natural, esa última es llamada *responsable del tratamiento*, para realizar el tratamiento directamente o entregarlo a un tercero que lo realice, llamado *encargado del tratamiento*.

Modelo europeo

Inicialmente el modelo europeo ubicó la protección de datos personales en el derecho privado como parte de los derechos de la personalidad, para trasladarse al derecho público cuando lo reconocen en las Constituciones de diversos países europeos de manera indirecta o directa como Derecho Fundamental: en Alemania con la Ley de Bonn a partir de interpretaciones de la dignidad humana y de manera expresa en la constitución portuguesa de 1976 en su artículo 26.1, por mencionar ejemplos. (Suárez Espino, 2008:68-69).

La revolución tecnológica empieza a acercar la información para ser tratada con fines decisivos en ámbitos comerciales, políticos, sociales, religiosos. En este preciso momento ante la gran cantidad de tecnologías disponibles para el tratamiento y el interés en la tutela que como garantía de la igualdad, el desarrollo de la personalidad y la dignidad humana, el modelo europeo adopta una actitud más activa y regula mediante leyes generales que asignan la función de controlar y limitar toda base de datos a una autoridad pública equivalente al Ombudsman sueco. El derecho al habeas data es denominado como derecho a la libertad informática.

La Directiva mencionada reconoce el derecho de las personas en relación con sus datos personales (Artículos 12, 14, 15), hace explícita en algunas partes de su articulado la necesidad de unos medios para garantizar su efectiva aplicación (Artículo 22 a 24), enunciados que se ven reforzados por los argumentos de sus consideraciones N°10,23, 25, 38, 41, 45,48, 52, 55, 61 , 62 y 63; donde puede concluirse que los estados deben promover y garantizar el lícito tratamiento de los datos personales y fijar procedimientos para que las personas puedan ejercer sus derechos de acceso, oposición, cancelación y rectificación ante la autoridad pública o personas privadas.

Modelo norteamericano

En el modelo norteamericano existe la dificultad de una ausencia en el reconocimiento del derecho a la intimidad, por lo cual la jurisprudencia se encargó de construir la noción de *privacy* a partir del antecedente del *Right to privacy* de Samuel Warren y Louis Brandeis, quienes concibieron el derecho a la intimidad como un “derecho a no ser molestado”, dentro de los derechos a la propiedad. La posición de la jurisprudencia ha sido eminentemente a favor del individuo frente a injerencias externas (Suárez Espino, 2008:58-61). El modelo norteamericano lo concibe como parte de una libertad civil, a partir de las Enmiendas VI y IX de la Constitución de 1787, que protege la esfera privada

El reconocimiento de la naturaleza espiritual del hombre amplió la aplicación del a) derecho a la vida, con la protección de intromisiones externas como la protección contra olores y b) del derecho a la propiedad, con la creación de una tutela jurídica sobre cosas inmateriales. Las nuevas invenciones que capturan aspectos de la vida personal de los Americanos son la situación perfecta que justifica la necesidad del “*right to be let alone*” para garantizar la *inviolate personality* (Warren & Brandeis, 1891).

El modelo norteamericano ha sido más pragmático, enfatizando en que es la autonomía del individuo la que debe decidir acerca de la información que pueden tratar de él o lo que se puede compartir, por lo cual no puede inmiscuirse el gobierno ni los particulares. Por ello los

conflictos o violaciones al derecho a la intimidad son dirimidos en los tribunales a través de la *tort liability* (PerezLuño, 2005:334) que es la acción de responsabilidad civil por cometer actos ilícitos que Prosser (1960:389) agrupa en 1) Intromisión en la esfera o en los asuntos privados ajenos, 2) Divulgación pública de hechos embarazosos de carácter privado, 3) Divulgación de hechos que suscitan una falsa imagen para el interesado a los ojos de la opinión pública, 4) Apropiación indebida para provecho propio del nombre e imagen ajenos.

Para efectos del derecho a la intimidad de los datos personales cabrían los numerales 1, 2 y 3, tomando como guía la definición que se da de dato personal y tratamiento de la información que explican los ámbitos de la *privacy* en el derecho norteamericano.

El modelo norteamericano considera la protección de datos personales como algo exclusivo del individuo y sus relaciones comerciales y civiles.

Regulación jurídica en Colombia

En Colombia antes del reconocimiento como derecho fundamental constitucional existieron normas que regularon el tratamiento y circulación de la información, principalmente mediante decretos reglamentarios y algunas leyes sectoriales (Remolina-Angarita, 2010a: p.505-508). Posterior a la vigencia del artículo 15 de la Carta Magna, la Corte Constitucional se encargó de regular vía jurisprudencia el habeas data hasta el año 2012 en que se expide una normativa integral y general sobre el habeas data.

La sentencia que inició la línea jurisprudencial sobre el tema, luego de su reconocimiento constitucional, fue la T-414 de 1992. En ella merece destacarse la procedibilidad de la acción de tutela como mecanismo de protección jurídica, el reconocimiento de la informática como un poder suficiente para afectar la intimidad, el requisito de “(...)lograr un justo equilibrio en la distribución del poder de la información y no exclusivamente, como en el pasado, a garantizar los apetitos de soledad de una persona” (Corte Constitucional, Sentencia T-414 de 1992, Magistrado Ponente Ciro Angarita Barón) y la necesidad de tutela jurídica ante los riesgos que genere a consecuencia de la “propiedad” del

dato almacenado en las bases de datos, que se resume la expresión de “encarcelamiento del alma en la sociedad contemporánea(...)”(Corte Constitucional, Sentencia T-414 de 1992, Magistrado Ponente Ciro Angarita Barón)

Colombia cuenta a nivel de regulación normativa con los artículos 15 Constitucional, la jurisprudencia constitucional vinculante, las leyes 12666 de 2008 sectorial (dato financiero, crediticio y comercial) y 1561 de 2012 estatutaria de protección de datos personas y diversas leyes ordinarias vigentes, y respecto a los medios para garantizar la aplicación de estas normas la principal ha sido la acción de tutela.

La ley 1581 de 2012 crea otros mecanismos administrativos como la consulta, el reclamo y la queja ante la autoridad de control ignorando otros, de los que la doctrina se pronuncia, como acción procesal especial habeas data, los códigos deontológicos, el agente de control interno, las tecnologías de protección de la privacidad y los acuerdos contractuales(Cerda, 2006, P.237-250.)(Remolina-Angarita, 2010b), así como también existen tipos penales específicos creados por la ley 1273 de 2009 para proteger este bien jurídico.

Estudios sobre los mecanismos de protección jurídica en otros contextos

El Profesor Nelson Remolina-Angarita (2010a, p.500) menciona que para analizar el grado de protección jurídica adecuado de los datos personales es preciso: i) el contenido material de la regulación normativa del derecho y ii) los medios para garantizar su efectiva aplicación.

La protección jurídica efectiva de la intimidad ha sido tratada por varios autores jurídicos, preocupados del impacto de las tecnologías creadas en la automatización de la recolección de la información personal que se comparte y proponiendo soluciones para incrementar la protección jurídica de las personas.

La información encontrada es el resultado del análisis sobre el desarrollo en forma gradual de la normatividad para protección de datos: comenzando con la revisión crítica de

las leyes surgidas para el control de la recolección y almacenamiento hasta terminar en las leyes más recientes que abogan por dar mayor papel a las personas de quienes extraen la información las empresas o instituciones gubernamentales.

Existen cinco alternativas jurídicas para regular la información personal: disposiciones constitucionales, leyes generales, leyes sectoriales, la contratación y la autorregulación. Las dos primeras han generado el modelo europeo y las tres últimas se presentan con mayor frecuencia en Norteamérica. Sin embargo hasta estos modelos han comenzado a tener influencias recíprocas de tal forma que usan instrumentos heterónomos y autónomos de regulación. Para efectos de este trabajo se dividen en dos los *sistemas de protección de datos personales*: a) europeo y b) norteamericano.

Sobre el contenido material del derecho protección de datos personales hay varios artículos científicos y publicaciones al respecto. Destacado el estudio de Alberto Cerda (2003: 54 y ss.) *Autodeterminación informativa y leyes sobre protección de datos*, que expone los desarrollos sustanciales del derecho al debido tratamiento de datos personales: desde su origen, dentro de la esfera del derecho a la intimidad o privacidad, hasta su independencia actual, en que se tienen regulaciones propias dadas las actuales circunstancias tecnológicas y sociales. Su planteamiento más destacable es que las nuevas tecnologías han impactado en la concepción pasiva del derecho a la intimidad (derecho a no ser molestado), transformándola en una más activa y especializada, que otorga un poder de control a las personas sobre aquello que desea compartir de ellos; además menciona las leyes que se enfocaron en regular el procedimiento de recolección y tratamiento de la información personal.

A nivel europeo se encuentran los documentos del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE de 1995 de la Comisión Europea sobre el tratamiento de datos personales, que orientan acerca de la evaluación de los países fuera de la comunidad europea para el cumplimiento adecuado de los estándares de la Directiva 95/46/CE de 1995. Sobre el tema objeto de esta investigación a nivel internacional se han encontrado dos documentos de la Comisión Europea (CE) acerca de la importancia de los mecanismos de protección de datos personales y un artículo que describe cuales son los mecanismos que imperan en Europa.

Los documentos de la CE de trabajo “Primeras orientaciones sobre la transferencia de datos personales a países de terceros – Posibles formas de evaluar la adecuación” (1998) y “Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE” (1998), presentan la definición de aquello que constituye *protección adecuada* de los datos personales; los elementos que conforman la protección adecuada, como son las leyes específicas a protección de las personas y los instrumentos o procedimientos para la aplicación efectiva; el checklist mínimo de protección adecuada que deben cumplir terceros países para permitir la transferencia de datos de ciudadanos europeos.

En Latinoamérica se encontraron tres artículos que analizan el Habeas Data en los ordenamientos jurídicos de varios países así como los mecanismos para la protección de datos personales.

El primero de ellos es del profesor venezolano Gonzalo Pérez Salazar, titulado “Naturaleza jurídica del Habeas Data” (en Velandia, 2013:681-710) y tiene como foco principal responder a la siguiente inquietud: ¿El Habeas Data en Venezuela debe concebirse como derecho fundamental, proceso judicial administrativo o recurso? para ello hace un análisis normativo de las constituciones y leyes de Colombia, Argentina, Perú, Ecuador y la Unión Europea. Este artículo presenta conclusión que el Habeas Data es el procedimiento constitucional para garantizar el derecho fundamental de protección de datos personales, luego de examinar múltiples tesis que lo conciben como recurso, garantía, derecho fundamental; de manera implícita deja ver la importancia de las vías procesales para hacer efectivo el derecho.

El segundo titulado “Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de habeas data en América Latina. Un intento clasificador con fines didácticos” del profesor Oscar Pucinelli (2004, 471-501), defiende la necesidad de una protección jurídica frente a las nuevas tecnologías en su aplicación a la recolección y tratamiento de datos personales, para ello concibe el derecho a la protección de datos personales como un derecho instrumental neto, así lo justifica porque lo protegido son los

derechos que se lesionen con el tratamiento indebido como el honor, la intimidad, el buen nombre, la libertad informativa o autodeterminación, aunque su tesis principal es que, como conjunto de reglas, derechos y normas, forman una nueva rama del derecho centrada en el debido o indebido tratamiento de datos personales; propone unos criterios para la elaboración de su clasificación del habeas data en Latinoamérica como son: la legitimación por activa, momento de incoarse la acción, la tutela de los derechos, el radio de acción y la finalidad perseguida.

El tercer estudio titulado “Mecanismos de control en la protección de datos en Europa”, del profesor Alberto Cerda, describe el desarrollo histórico de la legislación sobre protección de datos personales hasta la culminación en una última fase con la creación de los mecanismos para la protección de datos personales a través de una norma comunitaria europea bajo la justificación de otorgar garantías para el derecho efectivo a la autodeterminación informativa; los derechos de los titulares de los datos personales; los mecanismos contemplados en la Directiva 95/46/CE son: el agente de control interno, la autoridad administrativa de control, el código deontológico, tecnologías de protección de la intimidad, los contratos acuerdo, la responsabilidad civil objetiva, el control jurisdiccional por medio de acciones procesales o medida cautelar al titular del dato, sanciones, habeas data (como mecanismo específico y expedito para exigir protección mediante el sistema judicial y el procedimiento que se impulsa dentro de este) y el defensor del pueblo.

Sobre estudios realizados al respecto de los mecanismos jurídicos para la protección de datos personales en Colombia no se encontraron antecedentes al respecto. Sin embargo a continuación se mencionan los relacionados con la protección de datos personales.

Se destaca el artículo del profesor Nelson Remolina Angarita (2010, 489-524) que retoma los planteamientos realizados en los documentos europeos precitados y se propone analizar el grado de protección jurídica de la norma 1266 de 2006 del ordenamiento jurídico colombiano, enfocándose en el contenido material de la norma mencionada.

El trabajo del profesor Nelson Remolina-Angarita desplegado sobre la temática del Habeas Data en Colombia se muestra como el principal antecedente macro a nivel nacional porque ha trabajado de manera sistemática el desarrollo del Habeas Data en Colombia, comenzando con su trabajo de grado que estudió la regulación del Habeas Data en Colombia.

Bases legales

Constitución Política de 1991

(...)

ARTICULO 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 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.

(...)

Ley 1266 de 2008

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

ARTÍCULO 1°. OBJETO. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la

información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

(...)

ARTÍCULO 6o. DERECHOS DE LOS TITULARES DE LA INFORMACIÓN. Los titulares tendrán los siguientes derechos:

1. Frente a los operadores de los bancos de datos:

1.1 Ejercer el derecho fundamental al hábeas data en los términos de la presente ley, mediante la utilización de los procedimientos de consultas o reclamos, sin perjuicio de los demás mecanismos constitucionales y legales.

1.2 Solicitar el respeto y la protección de los demás derechos constitucionales o legales, así como de las demás disposiciones de la presente ley, mediante la utilización del procedimiento de reclamos y peticiones.

1.3 Solicitar prueba de la certificación de la existencia de la autorización expedida por la fuente o por el usuario.

1.4 Solicitar información acerca de los usuarios autorizados para obtener información.

PARÁGRAFO. La administración de información pública no requiere autorización del titular de los datos, pero se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la presente ley.

La administración de datos semiprivados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero, crediticio, comercial, de servicios y el proveniente de terceros países el cual no requiere autorización del titular. En

todo caso, la administración de datos semiprivados y privados se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la presente ley.

2. Frente a las fuentes de la información:

2.1 <Numeral CONDICIONALMENTE exequible> Ejercer los derechos fundamentales al hábeas data y de petición, cuyo cumplimiento se podrá realizar a través de los operadores, conforme lo previsto en los procedimientos de consultas y reclamos de esta ley, sin perjuicio de los demás mecanismos constitucionales o legales.

2.2 Solicitar información o pedir la actualización o rectificación de los datos contenidos en la base de datos, lo cual realizará el operador, con base en la información aportada por la fuente, conforme se establece en el procedimiento para consultas, reclamos y peticiones.

2.3 Solicitar prueba de la autorización, cuando dicha autorización sea requerida conforme lo previsto en la presente ley.

3. Frente a los usuarios:

3.1 Solicitar información sobre la utilización que el usuario le está dando a la información, cuando dicha información no hubiere sido suministrada por el operador.

3.2 Solicitar prueba de la autorización, cuando ella sea requerida conforme lo previsto en la presente ley.

PARÁGRAFO. Los titulares de información financiera y crediticia tendrán adicionalmente los siguientes derechos:

Podrán acudir ante la autoridad de vigilancia para presentar quejas contra las fuentes, operadores o usuarios por violación de las normas sobre administración de la información financiera y crediticia.

Así mismo, pueden acudir ante la autoridad de vigilancia para pretender que se ordene a un operador o fuente la corrección o actualización de sus datos personales, cuando ello sea procedente conforme lo establecido en la presente ley.

(...)

ARTÍCULO 10. PRINCIPIO DE FAVORECIMIENTO A UNA ACTIVIDAD DE INTERÉS PÚBLICO. La actividad de administración de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países está directamente relacionada y favorece una actividad de interés público, como lo es la actividad financiera propiamente, por cuanto ayuda a la democratización del crédito, promueve el desarrollo de la actividad de crédito, la protección de la confianza pública en el sistema financiero y la estabilidad del mismo, y genera otros beneficios para la economía nacional y en especial para la actividad financiera, crediticia, comercial y de servicios del país.

PARÁGRAFO 1o. La administración de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, por parte de fuentes, usuarios y operadores deberán realizarse de forma que permita favorecer los fines de expansión y democratización del crédito. Los usuarios de este tipo de información deberán valorar este tipo de información en forma concurrente con otros factores o elementos de juicio que técnicamente inciden en el estudio de riesgo y el análisis crediticio, y no podrán basarse exclusivamente en la información relativa al incumplimiento de obligaciones suministrada por los operadores para adoptar decisiones frente a solicitudes de crédito.

La Superintendencia Financiera de Colombia podrá imponer las sanciones previstas en la presente ley a los usuarios de la información que nieguen una solicitud de crédito basados exclusivamente en el reporte de información negativa del solicitante.

PARÁGRAFO 2o. La consulta de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países por parte del titular, será gratuita al menos una (1) vez cada mes calendario.(...)

TITULO V. PETICIONES DE CONSULTAS Y RECLAMOS.

ARTÍCULO 16. PETICIONES, CONSULTAS Y RECLAMOS.

I. Trámite de consultas. Los titulares de la información o sus causahabientes podrán consultar la información personal del titular, que repose en cualquier banco de datos, sea este del sector público o privado. El operador deberá suministrar a estos, debidamente identificados, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.

La petición, consulta de información se formulará verbalmente, por escrito, o por cualquier canal de comunicación, siempre y cuando se mantenga evidencia de la consulta por medios técnicos.

La petición o consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la petición o consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

PARÁGRAFO. La petición o consulta se deberá atender de fondo, suministrando integralmente toda la información solicitada.

II. Trámite de reclamos. Los titulares de la información o sus causahabientes que consideren que la información contenida en su registro individual en un banco de datos debe ser objeto de corrección o actualización podrán presentar un reclamo ante el operador, el cual será tramitado bajo las siguientes reglas:

1. La petición o reclamo se formulará mediante escrito dirigido al operador del banco de datos, con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y si fuere el caso, acompañando los documentos de soporte que se quieran hacer valer. En caso de que el escrito resulte incompleto, se deberá oficiar al interesado para que subsane las fallas. Transcurrido un mes desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido de la reclamación o petición.

2. Una vez recibido la petición o reclamo completo el operador incluirá en el registro individual en un término no mayor a dos (2) días hábiles una leyenda que diga “reclamo en trámite” y la naturaleza del mismo. Dicha información deberá mantenerse hasta que el reclamo sea decidido y deberá incluirse en la información que se suministra a los usuarios.

3. El término máximo para atender la petición o reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender la petición dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su petición, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

4. En los casos en que exista una fuente de información independiente del operador, este último deberá dar traslado del reclamo a la fuente en un término máximo de dos (2) días hábiles, la cual deberá resolver e informar la respuesta al operador en un plazo máximo de diez (10) días hábiles. En todo caso, la respuesta deberá darse al titular por el operador en el término máximo de quince (15) días hábiles contados a partir del día siguiente a la fecha de presentación de la reclamación, prorrogables por ocho (8) días hábiles más, según lo indicado en el numeral anterior. Si el reclamo es presentado ante la fuente, esta procederá a resolver directamente el reclamo, pero deberá informar al operador sobre la recepción del reclamo

dentro de los dos (2) días hábiles siguientes a su recibo, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga “reclamo en trámite” y la naturaleza del mismo dentro del registro individual, lo cual deberá hacer el operador dentro de los dos (2) días hábiles siguientes a haber recibido la información de la fuente.

5. Para dar respuesta a la petición o reclamo, el operador o la fuente, según sea el caso, deberá realizar una verificación completa de las observaciones o planteamientos del titular, asegurándose de revisar toda la información pertinente para poder dar una respuesta completa al titular.

7. Sin perjuicio del ejercicio de la acción de tutela para amparar el derecho fundamental del hábeas data, en caso que el titular no se encuentre satisfecho con la respuesta a la petición, podrá recurrir al proceso judicial correspondiente dentro de los términos legales pertinentes para debatir lo relacionado con la obligación reportada como incumplida. La demanda deberá ser interpuesta contra la fuente de la información la cual, una vez notificada de la misma, procederá a informar al operador dentro de los dos (2) días hábiles siguientes, de forma que se pueda dar cumplimiento a la obligación de incluir la leyenda que diga “información en discusión judicial” y la naturaleza de la misma dentro del registro individual, lo cual deberá hacer el operador dentro de los dos (2) días hábiles siguientes a haber recibido la información de la fuente y por todo el tiempo que tome obtener un fallo en firme. Igual procedimiento deberá seguirse en caso que la fuente inicie un proceso judicial contra el titular de la información, referente a la obligación reportada como incumplida, y este proponga excepciones de mérito.(...)

ARTÍCULO 17. FUNCIÓN DE VIGILANCIA. <Artículo CONDICIONALMENTE exequible> La Superintendencia de Industria y Comercio ejercerá la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales que se regula en la presente ley.

En los casos en que la fuente, usuario u operador de información sea una entidad vigilada por la Superintendencia Financiera de Colombia, esta ejercerá la vigilancia e impondrá las sanciones correspondientes, de conformidad con las facultades que le son propias, según lo establecido en el Estatuto Orgánico del Sistema Financiero y las demás normas pertinentes y las establecidas en la presente ley.

Para el ejercicio de la función de vigilancia a que se refiere el presente artículo, la Superintendencia de Industria y Comercio y la Superintendencia Financiera de Colombia, según el caso, tendrán en adición a las propias las siguientes facultades:

1. Impartir instrucciones y órdenes sobre la manera como deben cumplirse las disposiciones de la presente ley relacionadas con la administración de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países fijar los criterios que faciliten su cumplimiento y señalar procedimientos para su cabal aplicación.

2. Velar por el cumplimiento de las disposiciones de la presente ley, de las normas que la reglamenten y de las instrucciones impartidas por la respectiva Superintendencia.

3. Velar porque los operadores y fuentes cuenten con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley.

4. Ordenar a cargo del operador, la fuente o usuario la realización de auditorías externas de sistemas para verificar el cumplimiento de las disposiciones de la presente ley.

5. Ordenar de oficio o a petición de parte la corrección, actualización o retiro de datos personales cuando ello sea procedente, conforme con lo establecido en la presente ley. Cuando sea a petición de parte, se deberá acreditar ante la Superintendencia que se surtió el trámite de un reclamo por los mismos hechos ante el operador o la fuente, y que el mismo no fue atendido o fue atendido desfavorablemente.

6. Iniciar de oficio o a petición de parte investigaciones administrativas contra los operadores, fuentes y usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, con el fin de establecer si existe responsabilidad administrativa derivada del incumplimiento de las disposiciones de la presente ley o de las órdenes o instrucciones impartidas por el organismo de vigilancia respectivo, y si es del caso imponer sanciones u ordenar las medidas que resulten pertinentes.

Ley 1581 de 2012

Por la cual se dictan disposiciones generales para la protección de datos personales

ARTÍCULO 1o. OBJETO. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

ARTÍCULO 8o. DERECHOS DE LOS TITULARES. El Titular de los datos personales tendrá los siguientes derechos:

a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;

b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;

c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;

e) <Literal CONDICIONALMENTE exequible> Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;

TÍTULO V.

PROCEDIMIENTOS.

ARTÍCULO 14. CONSULTAS. Los Titulares o sus causahabientes podrán consultar la información personal del Titular que repose en cualquier base de datos, sea esta del sector público o privado. El Responsable del Tratamiento o Encargado del Tratamiento deberán suministrar a estos toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular.

La consulta se formulará por el medio habilitado por el Responsable del Tratamiento o Encargado del Tratamiento, siempre y cuando se pueda mantener prueba de esta.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

PARÁGRAFO. Las disposiciones contenidas en leyes especiales o los reglamentos expedidos por el Gobierno Nacional podrán establecer términos inferiores, atendiendo a la naturaleza del dato personal.

ARTÍCULO 15. RECLAMOS. El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley, podrán presentar un reclamo ante el Responsable del Tratamiento o el Encargado del Tratamiento el cual será tramitado bajo las siguientes reglas:

1. El reclamo se formulará mediante solicitud dirigida al Responsable del Tratamiento o al Encargado del Tratamiento, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quiera hacer valer. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

En caso de que quien reciba el reclamo no sea competente para resolverlo, dará traslado a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al interesado.

2. Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

ARTÍCULO 16. REQUISITO DE PROCEDIBILIDAD. El Titular o causahabiente sólo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento.

TÍTULO VI.

DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO.

ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
- b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;
- c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
- d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
- e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;

f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;

l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

m) Informar a solicitud del Titular sobre el uso dado a sus datos;

n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

ARTÍCULO 18. DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;

d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;

e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;

f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;

g) Registrar en la base de datos la leyenda “reclamo en trámite” en la forma en que se regula en la presente ley;

h) Insertar en la base de datos la leyenda “información en discusión judicial” una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;

i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;

k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;

l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

PARÁGRAFO. En el evento en que concurren las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno.

TÍTULO VII.

DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN.

CAPÍTULO I.

DE LA AUTORIDAD DE PROTECCIÓN DE DATOS.

ARTÍCULO 19. AUTORIDAD DE PROTECCIÓN DE DATOS. <Artículo CONDICIONALMENTE exequible> La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.

PARÁGRAFO 1o. El Gobierno Nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la

Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos.

PARÁGRAFO 2o. La vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma.

(...)

ARTÍCULO 21. FUNCIONES. La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:

a) Velar por el cumplimiento de la legislación en materia de protección de datos personales;

b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;

c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva;

d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos;

e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley;

f) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones.

g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos;

h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento;

i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional;

j) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personales;

k) Las demás que le sean asignadas por ley.

ARTÍCULO 27. NORMAS CORPORATIVAS VINCULANTES. El Gobierno Nacional expedirá la reglamentación correspondiente sobre Normas Corporativas Vinculantes para la certificación de buenas prácticas en protección de datos, personales y su transferencia a terceros países.

LEY 1273 DE 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

ARTÍCULO 1o. Adiciónase el Código Penal con un Título VII BIS denominado “De la Protección de la información y de los datos”, del siguiente tenor:(...)

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

(...)

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie,

envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

Ley 57 de 1887

“Sobre adopción de códigos y unificación de la legislación nacional.”

Código Civil Colombiano

ARTICULO 1o. Regirán en la República, noventa días después de la publicación de esta Ley, con las adiciones y reformas de que ella trata, los Códigos siguientes:

El Civil de la Nación, sancionado el 26 de Mayo de 1873;(…)

ARTICULO 63. CULPA Y DOLO. La ley distingue tres especies de culpa o descuido.

Culpa grave, negligencia grave, culpa lata, es la que consiste en no manejar los negocios ajenos con aquel cuidado que aun las personas negligentes o de poca prudencia suelen emplear en sus negocios propios. Esta culpa en materias civiles equivale al dolo.

Culpa leve, descuido leve, descuido ligero, es la falta de aquella diligencia y cuidado que los hombres emplean ordinariamente en sus negocios propios. Culpa o descuido, sin otra calificación, significa culpa o descuido leve. Esta especie de culpa se opone a la diligencia o cuidado ordinario o mediano.

El que debe administrar un negocio como un buen padre de familia, es responsable de esta especie de culpa.

Culpa o descuido levísimo es la falta de aquella esmerada diligencia que un hombre juicioso emplea en la administración de sus negocios importantes. Esta especie de culpa se opone a la suma diligencia o cuidado.

El dolo consiste en la intención positiva de inferir injuria a la persona o propiedad de otro.

ARTICULO 1604. <RESPONSABILIDAD DEL DEUDOR>. El deudor no es responsable sino de la culpa lata en los contratos que por su naturaleza solo son útiles al acreedor; es responsable de la leve en los contratos que se hacen para beneficio recíproco de las partes; y de la levísima en los contratos en que el deudor es el único que reporta beneficio.

El deudor no es responsable del caso fortuito, a menos que se haya constituido en mora (siendo el caso fortuito de aquellos que no hubieran dañado a la cosa debida, si hubiese sido entregado al acreedor), o que el caso fortuito haya sobrevenido por su culpa.

La prueba de la diligencia o cuidado incumbe al que ha debido emplearlo; la prueba del caso fortuito al que lo alega.

Todo lo cual, sin embargo, se entiende sin perjuicio de las disposiciones especiales de las leyes, y de las estipulaciones expresas de las partes.(...)

ARTICULO 1613. <INDEMNIZACION DE PERJUICIOS>. La indemnización de perjuicios comprende el daño emergente y lucro cesante, ya provenga de no haberse cumplido la obligación, o de haberse cumplido imperfectamente, o de haberse retardado el cumplimiento.

Exceptúanse los casos en que la ley la limita expresamente al daño emergente.

ARTICULO 1614. <DAÑO EMERGENTE Y LUCRO CESANTE>. Entiéndese por daño emergente el perjuicio o la pérdida que proviene de no haberse cumplido la obligación o de haberse cumplido imperfectamente, o de haberse retardado su cumplimiento; y por lucro cesante, la ganancia o provecho que deja de reportarse a consecuencia de no haberse cumplido la obligación, o cumplido imperfectamente, o retardado su cumplimiento.(...)

ARTICULO 1616. <RESPONSABILIDAD DEL DEUDOR EN LA CAUSACION DE PERJUICIOS>. Si no se puede imputar dolo al deudor, solo es responsable de los perjuicios que se previeron o pudieron preverse al tiempo del contrato; pero si hay dolo, es responsable de todos los perjuicios que fueron consecuencia inmediata o directa de no haberse cumplido la obligación o de haberse demorado su cumplimiento.

La mora producida por fuerza mayor o caso fortuito, no da lugar a indemnización de perjuicios.

Las estipulaciones de los contratantes podrán modificar estas reglas.

(...)

ARTICULO 2341. <RESPONSABILIDAD EXTRA CONTRACTUAL>. El que ha cometido un delito o culpa, que ha inferido daño a otro, es obligado a la indemnización, sin perjuicio de la pena principal que la ley imponga por la culpa o el delito cometido.

(...)

ARTICULO 2347. <RESPONSABILIDAD POR EL HECHO PROPIO Y DE LAS PERSONAS A CARGO>. Toda persona es responsable, no sólo de sus propias acciones para el efecto de indemnizar el daño sino del hecho de aquellos que estuvieren a su cuidado.

Sistema teórico

Definición de variables

VARIABLE	DEFINICIÓN
Herramientas jurídicas para la protección de datos	Es un conjunto de competencias (en el sentido de Alexy, 1998:231-239) que permiten ejercer el control sobre el

personales	ejercicio de sus datos personales con el fin de comprobar, inspeccionar y acceder a ellos para verificar el cumplimiento de las normas y derechos reconocidos a las personas.
Estándares de protección de datos personales	<p>Conjunto de modelos de protección de datos personales que se encuentran disponibles para los países al momento de crear sus normativas. Los modelos de protección existente que lo conforman son: modelo norteamericano de protección de datos personales y modelo europeo de protección de datos personales.</p> <p>Cada uno de estos modelos para efectos del trabajo tienen la siguiente estructura común: los sujetos intervinientes (titular del derecho, responsable del tratamiento, encargado del tratamiento, autoridades públicas), un objeto tutelado jurídicamente (dato personal, bases de datos personales, no ser molestado sin permiso), hechos con consecuencias jurídicas (el tratamiento, la autorización) y los procesos, acciones procesales y actos jurídicos que enmarcan dicha relación y fijan los parámetros de tratamiento que configuran unos derechos, obligaciones y competencias de los sujetos.</p>
Nivel de Protección adecuado	Es el análisis cualitativo, basado en el realizado por el Consejo de Europa, sobre los principios mínimos que debe contener las regulaciones de un país, para que pueda realizar tratamientos de sus ciudadanos, mediante un permiso. Los dos elementos que mira para la calificación son: (i) contenido de las normas aplicables y ii) los medios para garantizar su efectiva aplicación. (ver CE, 1997:5 y CE, 1998:5)

Fuente: Camilo José Puello Rincón. Febrero, 2016

Operacionalización de variables

VARIABLE: Herramientas para la protección de datos personales de Colombia

DIMENSIONES	INDICADORES
Derecho de protección del dato personal	<ul style="list-style-type: none"> – Evolución histórica en el ordenamiento jurídico – Objeto de protección constitucional del derecho de protección de datos personales – Sujetos titulares del derecho de protección – Derechos del titular del dato personal – Derechos conexos – Encargados y responsables del tratamiento de datos personales
Mecanismos jurídicos para protección	<ul style="list-style-type: none"> – Mecanismos jurídicos – Mecanismos técnicos o tecnológicos
Tutela jurisdiccional	<ul style="list-style-type: none"> – Acción de tutela – Acción penal – Acción de responsabilidad civil – Habeas Data
Tutela administrativa	<ul style="list-style-type: none"> – Vigilancia de la Autoridad de protección de datos personales – Consulta – Reclamo – Queja – Defensor del Pueblo – Sanciones – Queja disciplinaria – Certificación
Autonomía privada	<ul style="list-style-type: none"> – Teoría de los derechos subjetivos – Códigos de conducta – Cláusulas contractuales – Agente de control interno

	<ul style="list-style-type: none"> – Contratos- acuerdo – Tecnologías de protección de la intimidad – Normas corporativas internacionales vinculantes
--	--

Fuente: Camilo José Puello Rincón, Febrero de 2016.

VARIABLE: Nivel de protección jurídica

DIMENSIONES	INDICADORES
Justificación para la protección jurídica	<ul style="list-style-type: none"> – Derecho de Habeas Data o autodeterminación informática – Protección derechos conexos – Protección de libertades públicas
Primer Requisito: Desarrollo normativo	<ul style="list-style-type: none"> – Convenios Internacionales – Convenios binacionales – Constitucionalización – Leyes nacionales generales – Leyes sectoriales
Segundo Requisito : Regulación de los mecanismos	<ul style="list-style-type: none"> - Claridad en los derechos del titular del dato protegidos - Diversidad de derechos protegidos al titular del dato
Tercer requisito: Presupuestos para Transferencias y recolección internacional de datos personales	<ul style="list-style-type: none"> – Internet – Bases de datos personales – Uso masivo de las TIC e intensificación en el uso de los datos personales – Políticas de privacidad – Pautas de transferencia – Principio de equivalencia normativa – Medidas de seguridad hacia el transferente – Ampliación del ámbito territorial de aplicación

Fuente: Camilo José Puello Rincón, Febrero de 2016.

VARIABLE: Estándares de Protección de Datos Personales

DIMENSIONES	INDICADORES
Modelo Europeo	<ul style="list-style-type: none"> – Derecho a la intimidad originado en la persona humana – Elementos importantes – Intereses jurídicos protegidos – Constitucionalización del derecho a la intimidad – Principios mínimos prevalecientes
Modelo Norteamericano	<ul style="list-style-type: none"> – Doctrina del derecho a la vida privada – Tutela indirecta – Criterios para identificar el caso de violación de privacy – Autoridades sectoriales – Uso amplio de los datos personales – Limitación temporal en conservación de datos personales – Principios mínimos prevalecientes

Fuente: Camilo José Puello Rincón, Febrero de 2016.

DISEÑO METODOLÓGICO

Tipo y método de investigación

La investigación es jurídica, descriptiva y aplicando el método de análisis sistemático y mental.

El tipo de investigación es jurídica (Giraldo, 2007:236) porque se desenvuelve alrededor de un tema específico: las fuentes formales del derecho, porque “(...) la confrontación no se hace contra la realidad empírica, sino contra las fuentes formales del Derecho” (Giraldo, 2007: 236) hay que buscar la respuesta en el ordenamiento jurídico, en las normas debidamente

interpretadas y criticadas. En esta investigación el objeto son los mecanismos para la protección jurídica de los datos personales en el ordenamiento jurídico vigente en Colombia.

La investigación es descriptiva, porque según Hernández Sampieri (2010:80) esta investigación consiste “(...) especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice” y en detalle las variables: mecanismos para la protección de datos personales en Colombia, estándares para la protección de datos personales en Colombia y nivel de protección jurídica.

El método de investigación es el *análisis sistemático y mental*, aplicable a los objetos del espíritu o que no tienen una existencia. Jacobo Pérez (2013:37) lo explica así: “Recorre a la abstracción en ciencias inmatrimales y los fenómenos suprasensibles, como la psicología, la historia, la sociología y el derecho”. El análisis se propone explicar las relaciones que existen entre elementos del modelo de protección de los Datos Personales, en especial la posición que ocupan los mecanismos dentro de cada modelo.

La técnica de investigación a utilizar es la documental porque la información será recolectada siguiendo los pasos establecidos que son “la búsqueda, el registro y la crítica de las fuentes del conocimiento jurídico, incluyendo en ella la mera búsqueda o información bibliografía” (Pérez, 2013:142) A partir de esta técnica de investigación saldrán los instrumentos para la recolección de la información.

Población y muestra

Por tratarse de una investigación jurídica y descriptiva, no se tomara una población específica como tal, sino estará basada en el análisis documental, jurisprudencial y normativo relacionado con la dogmática sobre los derechos a la intimidad, buen nombre, al Habeas Data, a la protección de datos personales

Análisis de información

Análisis documental

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR :	Camilo José Puello Rincón
	GUIA N° 01 de 22/02/2015
Propósito del diligenciamiento: Conocer a grandes rasgos el modelo europeo de protección de datos personales en su breve antecedente histórico, contado por una persona que se encuentra dentro del organismo europeo encargado de protección de datos.	
Referencia Bibliográfica	CERVERA NAVAS, Leonardo. El modelo europeo de protección de datos de carácter personal. <i>Cuadernos de Derecho Público</i> , [S.l.], may. 2011. ISSN 1989-8967. Disponible en: < http://revistasonline.inap.es/index.php?journal=CDP&page=article&op=view&path%5B%5D=694 >.
Tema	Modelos de protección de datos personales
Conceptos Clave	Privacy, Right to be alone, Protección de datos personales, intimidad, propiedad, autorregulación.
Idea principal	El derecho al tratamiento de datos personales surge en Estados Unidos a finales del siglo XIX y se desarrolla posteriormente en Europa a mitad del siglo XX.
Ideas secundarias relevantes	El derecho a la privacidad surge como una proyección existencial del derecho a la vida, es un to be let alone, a estar solo o no ser molestado o disfrutar la vida. El derecho a la privacidad comienza a ser tema público por el aumento de las tecnologías de vigilancia de las personas. Esa preocupación se palpa en la novela 1984 de George Orwell. El modelo estadounidense de privacidad, que en principio fue novedoso, se rezaga debido a la estructura del sistema jurídico del país; el concepto de privacidad derivada de otros derechos en la Constitución que se tienen, cuyo elemento esencial es que solo le incumbe proteger al individuo porque es una civil liberties; el desarrollo empresarial que hace lobby por evitar regulaciones más claras y expresas. Como críticas al modelo europeo se encuentran: naturaleza de derecho fundamental que limita la autodeterminación de la persona, que se ocupa de regular en forma general la protección y debe limitarse a leyes indemnizatorias de daños. El acercamiento entre los modelos es la autorregulación
Análisis conceptual del documento	El texto es una exposición muy dicente y corta del surgimiento histórico del derecho a la privacidad o la autodeterminación informativa. Luego se centra en analizar una crítica que se le hace al sistema europeo. Al final concluyendo como se percibe a lo largo del texto, que el sistema europeo es el más adecuado a las circunstancias actuales, dada la preocupación de los ciudadanos por la protección de su intimidad.
Aportes del texto	El aporte importante es la referencia a otros autores sobre el origen de la privacidad en el modelo estadounidense de protección de datos personales.
Polémicas	No se identifican polémicas o planteamientos.
Preguntas que suscita el texto	El texto es más descriptivo, tiene bastante claridad sobre el tema.
Comentario Personal	Es necesario profundizar en el origen del modelo europeo de protección de datos personales.
Referencia de otros autores	WARREN &BRANDEIS. The right to privacy. Harvard Law Review REGAN, Priscila. Legislating Privacy. Technology social values and public policy, Chapel Hill, 1995 Tribunal Constitucional Aleman. Sentencia del 15 de diciembre de 1983

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 02 de 22/07/2014
Propósito del diligenciamiento: Conocer los cambios en el desarrollo jurídico del derecho al autodeterminación informativa a través de regulaciones jurídicas internacionales(Alemania, Suecia, Francia, España, Italia, Finlandia) de diversos países y los nuevos fenómenos que se presentan relacionados con el uso intensivo de las nuevas tecnologías de la información y la comunicación.	
Referencia Bibliográfica	Cerda Silva, A. (Enero, 2003). Autodeterminación informativa y leyes sobre protección de datos. Revista Chilena de Derecho Informático, [S.l.], n. 3, ISSN 0717-9162. Disponible en: < http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/view/10661/11413 >. Fecha de acceso: 24 ene. 2016 doi:10.5354/0717-9162.2003.10661.
Tema	Derecho a la protección de datos personales y leyes sobre protección de datos.
Conceptos Clave	Derecho a la intimidad, autodeterminación informativa, <i>Safe Harbor Agreement</i> , liberalismo filosófico, <i>liberties pollution</i> , <i>safe harbor agreement</i> , teoría del mosaico.
Idea principal	Los cambios que sucedieron en la regulación jurídica del derecho al tratamiento de los datos personales, analizándolo conceptualmente así como también exponiendo las regulaciones que destacaron por cambios sustanciales al implementarse.
Ideas secundarias relevantes	<p>El derecho a la intimidad tiene su derecho en la premisa de la autonomía personal y la diferenciación de cada sujeto, teniendo todo el poder de elegir su vida sin ser molestado por el Estado, en principio y luego cualquier otro individuo, así se expone en las tesis de Benjamin CONSTANT.</p> <p>Por otra parte explica el origen conceptual del derecho a la privacidad a través de un análisis jurídico hecho por los autores norteamericanos Louis BRANDEIS y Samuel WARREN a partir del derecho a la propiedad. Luego viene su reconocimiento internacional en el artículo 12 de la Declaración de la ONU de 1948, declaración americana de los derechos del hombre, artículo 5; artículo 12 del Pacto de 1966; artículo 11 Convención Americana de los Derechos Humanos; artículo 16 Convención del niño de 1989.</p> <p>Las teorías jurídicas se han centrado en establecer cuáles son los márgenes de protección que brinda el derecho a la intimidad. Cita la teoría alemana de las esferas del individuo, donde hay aspectos lejanos al individuo, otros intermedios como el de la intimidad y uno cercano al sujeto que es el secreto o confidencialidad.</p> <p>Con los aportes teóricos de WESTIN y FRIED en los sesenta se concibe una privacidad más activa, que se centra en dar poder a la persona para controlar que información se ha recolectado de ella, dejando la concepción de prohibición de retener nuestros datos(The right to control information about oneself)</p> <p>El tema de la protección de los datos personales recogidos se debe a que las TIC han generado “una insospechada capacidad para recoger, procesar y transmitir información(...)” Esto ha suscitado la defensa de estudiosos que ven una posible vulneración a derechos fundamentales por acceder a información que permite conocer a las personas; por tanto debe estar al resguardo, y condicionar profundamente las libertades; incide también en la reformulación del concepto de derecho a la intimidad como un poder que tiene el sujeto para decidir “(...)cuanto de sí-pensamientos, sentimientos así como hechos de su vida personal- está dispuesto a compartir con los otros”(P.52 y ver siguiente párrafo)</p> <p>“El derecho a la autodeterminación informativa se construye a partir del derecho a la intimidad, que se fundamenta en el derecho de propiedad (...) la autodeterminación informativa no se circunscribe a amparar a la persona frente al tratamiento de datos personales que le conciernan y que le revelen circunstancias personales que le merezcan permanecer en la esfera privada (...) se extiende a todo dato que se predica de determinada persona.” (P.54)</p> <p>En España se trató en principio como libertad informática adscrito al derecho a la intimidad, porque la sentencia hito se pronunció sobre la recolección de datos por un programa de computador. Posteriormente se independizó la noción y sufrió una ampliación para abarcar todo dato recogido de la persona y almacenado en cualquier base de datos mecánica, informática o electrónica.</p>

	<p>La situación ha empezado a regularse por vía de ley debido al uso masivo de los dispositivos electrónicos, la informática y las telecomunicaciones, que permite almacenamiento, procesamiento y recuperación de la información contenida. En efecto la primera ley es del Land de Hesse, con el fin de regular la recolección y tratamiento de la información por parte de las administraciones públicas; Alemania a nivel federal promulga la Ley Federal de Protección de Datos Personales que incluye los mecanismos de derecho de bloqueo, tipificación penal de delitos, infracciones al tratamiento, autoridad federal de protección de datos a nivel público como también comisarios internos de protección de datos y autoridades de tutela estatal.</p> <p>En Suecia se profiere una ley en 1973 que asigna a una autoridad estatal la vigilancia del registro público de bancos de datos relativos a personas realizado por medios automatizados que autorizaba el funcionamiento de las bases de datos; se le conceden facultades inspectoras y procesales para aplicar judicialmente sanciones. La ley alemana y sueca impuso sanciones nuevas pero reconoció pocos derechos al titular de dato personal. Esta fue la primera generación de leyes.</p> <p>Posteriormente la tecnología avanzó y las nuevas leyes promulgadas flexibilizaron la operatividad de las bases de datos y concedieron derechos al titular de estos: información, acceso, rectificación y cancelación. Protegen el tratamiento de datos sensibles.</p> <p>La ley francesa innova al prohibir que se usen informaciones recopiladas en bases de datos contra la persona, así como también el derecho de esta a impugnar lo que se encuentre almacenado cuando se presente como prueba en procesos judiciales.</p> <p>Las normas de primera generación se centraron en regular la actividad de las bases de datos, mientras que la segunda se fijó en los datos y los derechos de los titulares. La tercera generación de normas se centra en el tratamiento de los datos personales, siendo ejemplo el Convenio 108 del Consejo Europeo.</p> <p>La Data Protection Act británica de 1984 establece los mecanismos de código de conducta, reglamentación especial y autoridad de control, Registrar, que puede tomar medidas cautelares y recibir las quejas, así como también un Data Protection Tribunal para que dirima el conflicto, que no menoscaba la competencia de los tribunales ordinarios</p> <p>La ley federal alemana de Protección de Datos de 1990, establece un sistema de responsabilidad civil objetiva, sin culpa y solidaria por los perjuicios causados por la elaboración automatizada de datos de un organismo público, pero al provenir de un ente no público “altera la carga de la prueba ante la controversia respecto del nexo causal de los perjuicios”(P.65).</p> <p>Ante la poca eficacia del Convenio 108 se fija la necesidad de expedir una Directiva comunitaria referente a los datos personales, es esta la 95/46/CE.</p> <p>En Estados Unidos la situación se deja la regulación sectorial y su cumplimiento a los interesados a través de códigos de conducta y ejercicio de sus derechos. Es un modelo de autorregulación y autocontrol.</p> <p>Ante este desacuerdo en los modelos de protección de los datos personales europeo y estadounidense, se negoció un acuerdo de puerto seguro (Safe Harbor Agreement) que toda entidad que trate datos personales de Europa debe aceptar, que se manifiestan en los principios de puerto seguro (Safe Harbor Principles).</p>
Análisis conceptual del documento	<ul style="list-style-type: none"> • El derecho a la intimidad es el antecesor del derecho a la autodeterminación informativa. Los primeros planteamientos surgen en los filósofos liberales que defienden un apartamiento del Estado hacia nosotros.

	<ul style="list-style-type: none"> • Jurídicamente el concepto de intimidad es formulado como un derecho para que cada individuo tenga su lugar “a solas” o privado. Así lo conciben Warren y Brandeis para protegerse de la invasión a su privacidad que representaban los nuevos medios de comunicación. • Su importancia es reconocida jurídicamente al darle la categoría de norma constitucional en las cartas fundamentales de varios estados y elevando su categoría en la Declaración Universal de los Derechos Humanos de la ONU. • Sin embargo hay dificultades en la época actual para determinar qué es lo íntimo y que no lo es. • La doctrina norteamericana centró su análisis en proponer un papel más activo del derecho a la intimidad para formularlo como un derecho de control y acceso a la información de nosotros. Quien, qué, cómo, para qué, por cuanto tiempo se tiene nuestra información. • La evolución de la regulación jurídica del tratamiento de datos personales ha pasado por 3 etapas: la fundamentación en el derecho a la intimidad (prohibición de ser molestado arbitrariamente en su intimidad), luego independizándose, al concebirse como conjunto de facultades de autodeterminación de la información personal para enfrentar riesgos inherentes a tal autorización, y finalmente, pasar a diseñarse de manera instrumental como derecho para el control del debido tratamiento de los datos personales. • Descripción de las normativas adoptadas a nivel internacional sobre tratamiento de datos personales y flujo multinacional de datos, así como las herramientas para vigilar su cumplimiento. • La primera fase de las legislaciones se centraron en realizar controles previos para dar permisos para tratamiento a través de las bases de datos y una autoridad pública que supervisa la efectividad de la normativa. • En la ley federal alemana de protección de datos personales de 1977 se consagra el derecho de bloqueo del dato personal para evitar su uso más allá del que realiza el tratamiento, la tipificación de nuevos delitos y la creación de un agente de control interno en cada entidad tratante llamado <i>comisario de protección de datos personales</i>. • En la anteriormente citada ley alemana destaca el régimen de inspección y vigilancia doble sobre cumplimiento de la normativa: público y privado. Para el sector estatal se asigna el deber de reglamentar administrativamente y una autoridad pública especial para eso llamada <i>Comisario Federal de Protección de Datos</i> y para el sector privado el agente interno y la autoridad pública estatal mencionada anteriormente. • Suecia innova en su legislación con la creación de un registro nacional de bases de datos. • La segunda generación de normas promulgadas se centran en el individuo, dándole más poder para ejercer sus derechos debido a la facilidad técnica que se vuelve construir una base de datos por el aumento en la capacidad de cómputo y almacenamiento, derechos de acceso, oposición, cancelación y rectificación; se inicia el debate sobre ciertos datos sensibles por pertenecer a sujetos de especial protección como los menores de edad, sindicalistas, miembros de partidos políticos y periodistas; se crea prohibiciones para tomar decisiones jurídicas y jurisdiccionales con base única en el dato personal. Ejemplo de ello son las leyes francesa de 1978 y la estadounidense de 1974 Privacy Act, a nivel internacional están el convenio 108 de la Union Europea, la resolución de la ONU sobre tratamiento de ficheros computacionales y la resolución de la OCDE sobre directrices aplicables a la protección de la vida privada en los flujos transfronterizos de datos personales. • La legislación británica innova al crear otros mecanismos de regulación como los códigos de
--	---

	<p>conducta que son para autorregulación de los particulares, así como una autoridad administrativa, el <i>Registrar</i> y una autoridad judicial el <i>Data Protection Tribunal</i> encargado de ser segunda instancia del anterior.</p> <ul style="list-style-type: none"> • La legislación europea actualiza se actualiza con la Directiva 95/46/CE, cuya novedad es el énfasis en cumplir con la calidad del dato personal, es decir, que este actualizado y vigente, se asocia la legitimidad del consentimiento previo de tratamiento con la finalidad prevista, la publicidad del tratamiento ante la autoridad pública por parte del responsable, la obligación a sus miembros de crear un recurso judicial específico. La más grande contribución fue la creación del concepto de <i>nivel adecuado de protección</i> para proteger a las personas del flujo transfronterizo de datos hacia países que no tienen una normativa fuerte. • Los acuerdos que llegaron la Unión Europea y los Estados Unidos de América para poder realizar transferencias internacionales de datos recíprocamente se llaman <i>Safe Harbor Principles</i>.
Aportes del texto	<p>Con la lectura del texto surgieron las preguntas acerca de los fundamentos jurídicos y filosóficos del derecho al habeas data o autodeterminación informativa, que se piensa como una de las secciones de la investigación.</p> <p>También ayudó el análisis que hace al desarrollo del derecho a la autodeterminación informática desde la perspectiva de las leyes que desarrolló el legislador americano y europeo</p>
Polémicas	<p>¿Qué aspectos deben calificarse como íntimos? Hay tres teorías según la espacialidad, el sujeto o acorde a la naturaleza de los acontecimientos.</p> <p>¿La protección frente al tratamiento de los datos personales constituye una expresión de un derecho ya existente cual es el derecho a la intimidad, o bien representa una nueva categoría de derecho, que garantiza a la persona facultades de información, acceso y control de los datos que le conciernen? (Caso de la jurisprudencia de la Suprema Corte de EE.UU. sobre privacy que se extiende al tratamiento de los datos personales, en la jurisprudencia alemana autodeterminación informativa, en la italiana y española libertad informativa)</p>
Preguntas que suscita el texto	<p>¿Cuáles aspectos se tomaron del liberalismo filosófico para desarrollar el derecho a la intimidad?</p> <p>¿Existe una diferencia entre el derecho a la autodeterminación informativa y la libertad informativa?</p>
Comentario Personal	<p>El artículo destaca la evolución normativa de la protección del dato personal, iniciando con un énfasis en el dato personal y las diferenciaciones para tratarlo, pasando por los mecanismos adecuados de tratamiento de ellos (principios) y terminando en los derechos que se le reconocen a los titulares. Se pasó de un sistema pasivo a uno activo de habeas data.</p>
Referencia de otros autores	<p>BEJAR, Helena. El ámbito íntimo. Privacidad, individualismo y modernidad.</p> <p>BRANDES Y WARREN. The right to Privacy en Harvard Law Review, IV 1890.</p> <p>CONSTANT, Benjamin. De la libertad de los antiguos comparada con los modernos.</p> <p>HOBBS, Thomas. El leviatán.</p> <p>LOCKE, John. Segundo tratado del gobierno civil.</p> <p>MILL, John. Sobre la libertad.</p> <p>MURILLO DE LA CUEVA, Pablo. El derecho a la autodeterminación informativa. La protección de los datos personales frente a la informática. Tecnos, 1990</p> <p>PEREZ-LUÑO, Antonio. Derechos humanos, estado de derecho y constitución. Tecnos, 1995.</p> <p>WESTIN, Alan. Privacy and freedom. Atheneum, New York. 1967</p> <p>FRIED, Charles. Privacy. Yale law Journal, Vol.77.1968</p> <p>ONU. Principios rectores para la reglamentación de los ficheros computarizados de datos personales. Resolución 45 de 1995 de la ONU y Carta de los Derechos Fundamentales, artículo 7.</p>

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N°03 de 7/10/2014
El propósito de la lectura es la obtención del conocimiento básico acerca de los mecanismos existentes para proteger los datos personales en Europa, describiendo con especial énfasis en aquellos en los que está legitimado el titular del dato o la autoridad determinada contra el responsable del tratamiento.	
Referencia Bibliográfica	Cerda Silva, A. (Diciembre, 2006). Mecanismos de Control en la Protección de Datos en Europa. <i>Ius et Praxis</i> . Revista de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, núm. 12, 221-251.
Tema	Derechos Fundamentales, Derechos Humanos, Intimidación en la Constitución española, Intimidación bajo la informática.
Conceptos Clave	Ámbito de aplicación de las leyes, principios rectores, mecanismos de control, derechos, vida privada, datos personales, código de conducta.
Idea principal	La normativa que rige en Europa así como la de algunos países expone los aspectos que influyen en la concepción de los mecanismos, bien sea en cuanto a los principios que los impulsan o a los derechos que protegen. Es necesario que una autoridad pública fuerte para el control y vigilancia a los responsables y encargados del tratamiento de información personal.
Ideas secundarias relevantes	<p>Los países europeos han tenido presente la importancia de regular el campo del tratamiento de datos personales conforme avanzaba la tecnología procesadora de ellos, de esta manera se han identificado los siguientes períodos:</p> <p>En un primer período el objeto de la ley es brindar protección a las personas frente a la recolección y tratamiento de datos personales por las autoridades públicas y personas que ejercen funciones públicas que se amplía posteriormente al sector privado. (Ley Federal de Datos Alemana de 1977; se crea un registro público de bases de datos obligatorio para funcionar y una autoridad encargada de hacer cumplir mediante solicitud de sanciones judiciales (<i>Data Leg de 1973/289</i> de Suecia).</p> <p>En un segundo período, el objeto de las leyes flexibiliza la regulación sobre las entidades recolectoras y pone su lupa en las personas, confiriéndoles facultades para que sepan del debido tratamiento: acceso, cancelación, supresión, información como también en la normatividad sobre datos sensibles, como aquellos personales que al conocerse pueden conllevar una discriminación contra la persona o le lesionan su intimidad (Ley francesa de 1978. La causa fue el progreso de la informática y la creciente capacidad de almacenamiento de información.</p> <p>La Comunidad Europea al pasar los años concluye la necesidad de una norma que acerque la disparidad de criterios, tal idea se concreta en el Convenio 108 por la CEE en 1981 para la regulación del tratamiento automatizado de datos personales y el flujo internacional de ellos. Este convenio protegía a las personas naturales en la recolección, tratamiento y supresión de sus datos, también imponía el deber de adoptar las medidas necesarias para la efectividad del mismo, así se aprobaron: <i>Data Protection Act (1984)</i> del Reino Unido, Ley Orgánica de Regulación del Tratamiento Automatizado de Datos (LORTAD,1992) de España y la Ley</p>

Federal de Datos de Alemania en 1990. Posteriormente se adopta la directiva 95/46/CE porque el Convenio había mostrado poca eficacia en su adopción; Italia adopta la primera ley en 1996, *Ley 675 sobre la tutela de otras personas y otros sujetos respecto al tratamiento de datos personales*; el Reino Unido con la *Data Protection Act* de 1998; en España la ley de protección de datos de carácter personal. Esa directiva excluye a las personas jurídicas como sujetos de protección.

Hay una regulación homogénea en todos los países de la Unión Europea y se proyecta a terceros países. Sin embargo no se ha tenido en cuenta los derechos de los titulares de los datos personales, de tal manera que en un tercer período ha surgido una tendencia a constitucionalizar el derecho al tratamiento de datos personales. Portugal(1976), España(1978), Países Bajos(1983), Hungría(1989), Suecia(1993) y Finlandia(1999). De resaltar la Carta Europea de Derechos Humanos en sus artículos 7(derecho a la vida privada) y 8(derecho a la protección de los bienes de carácter personal). La Carta de Derechos fundamentales de la Unión Europea lo reconoce en su artículo 7 como un “derecho a la vida privada” y en su artículo 8 desprende la “protección de los bienes de carácter personal”, considerando los datos que le conciernen.

El Tribunal Constitucional alemán esboza el primigeniamente el derecho a la protección de datos personales como “derecho a la autodeterminación informativa” al pronunciarse sobre la ley del Censo de Población de 1982.

El marco principal que delimita el ámbito de aplicación es la directiva 95 y se proyecta a todo campo donde se verifique el tratamiento de datos personales, es la técnica legislativa *omni bus* (por el contrario a la de *by sector* de EE.UU.) Sin embargo la Unión Europea ha previsto las dificultades de aplicar una norma general en contextos específicos, así que ha proferido directivas para sectores determinados (Directiva 97/66/CE *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones*; Directiva 2002/58/CE, *relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas*)

Los estados europeos incorporaron a su legislación normas que hicieron efectivos los siguientes principios fundamentales: **calidad de los datos y lealtad en las operaciones de tratamiento sobre ellos; protección especial a los datos sensibles mediante excepciones, garantías y prohibiciones; medidas de seguridad física y lógica; derecho de acceso, rectificación y cancelación; garantía de un recurso a favor de quien fuere desestimada la petición formulada en ejercicio de sus derechos; licitud y lealtad(buena fe en la autorización para tratamiento); calidad de los datos(datos personales fidedignos que denotan),**

consentimiento informado(saber para qué fines se trata); seguridad de los datos(herramientas técnicas, físicas para proteger los datos de usos ilegales, ilícitos o no autorizados); confidencialidad de los datos (reserva de los datos para el responsable y quienes acceden), consentimiento en la cesión de datos(para transmitir a terceros), finalidad(los datos deben tener un propósito específico).

El titular del dato personal tiene los siguientes derechos: **acceso, información, rectificación, cancelación, oposición o bloqueo de datos, a impugnar decisiones adoptadas exclusivamente sobre la base del tratamiento automatizado de datos personales** (en la ley francesa de 1978), **derecho de acceso por medios indirectos**. También tiene el derecho a ser reparados por el responsable del tratamiento de datos personales si comete un tratamiento indebido, se excluye cuando ocurrió por responsabilidad del interesado o titular del dato o fuerza mayor.

La directiva europea establece un sistema de responsabilidad civil objetiva así como también por incumplimiento de las normas, se estipulan sanción penal o administrativa; la existencia del dolo o culpa para imputar la responsabilidad por indebido tratamiento dejaría sin piso el estándar común que fijo la directiva.

En España hay infracciones penales y otras con la aplicación de multa, en Francia se contemplan sanciones penales (p15): tratamiento de datos sin que medie acto habilitante o notificación previa a la Comisión, tratamiento ilegítimo y fraudulento de datos nominativos, divulgación sin autorización del titular de datos nominativos lesivos a la reputación, desviación de finalidad en el tratamiento de datos.

“El control (...) supone la concurrencia de dos elementos esenciales: existencia de un determinado estándar normativo conocido para el agente controlador como a quien se supervisa y el segundo, la formulación por el agente de control de un juicio de adecuación de la actividad de quien es controlado a tal patrón.” Ese patrón o estándar normativo se conjuga en los mecanismos de control que verifican el cumplimiento así como también la sanción por su incumplimiento, son preferiblemente judiciales, aunque no se omiten los administrativos como la autoridad pública o otros autónomos como los códigos de conducta y el agente de control interno (P.235, último párrafo)

Algunos países confieren a sus autoridades administrativas facultades que no exigen un requerimiento judicial previo, se les permite ordenar “medida cautelar al sistema de información, conferir o denegar la autorización a procesar datos, oponerse al registro de cierta

información suministrada por el responsable del tratamiento o dictaminar la implementación de medidas de seguridad.”(P.236) Pero para inspección judicial de un establecimiento que trata los datos o imposición de sanción se requiere orden judicial, “será la autoridad de control quien arrastrará al responsable de tratamiento a sede judicial” (P.236). Este artículo no excluye el estudio de las acciones judiciales que se conceden al responsable del tratamiento por las decisiones lesivas de la autoridad de control para restablecer los derechos a la protección de las personas.

La razón de ser de los mecanismos creados para el titular del dato es garantizar el derecho efectivo a la autodeterminación informativa, citando a Pérez Luño el autor fija en que hay una “procedualización del derecho moderno”. Siguiendo la anterior tónica algunos estados crean un procedimiento específico, concentrado y simplificado. La doctrina denomina *habeas data*, tomando prestado de *habeas corpus* algunas características, y hace referencia a la acción propiamente como al proceso que inicia el titular del dato. (Requerimiento de sus datos-reclamación administrativa-acción judicial).

Otro mecanismo es el **código deontológico** que se fija por una asociación sectorial o profesional que es pública, legal, obligatoria y legitimada en el medio que profiere el mismo (ver más P.21), fijando pautas de conducta que deben acatarse en el tratamiento de datos personales según fines diversos, porque representan una adecuación de las normas generales de los países y la directiva. Esta última lo fija así en el capítulo V. La importancia de estos códigos es que están adaptando normas generales y evitando que entren en obsolescencia, ahora de llegar esto último a ocurrir, juegan una gran influencia en la expedición de nuevas normas.

Los “códigos comunitarios” pueden someterse a la valoración del Grupo de la directiva, quien publicará aquellos que a su juicio estén conformes a los estándares de la directiva. Esos códigos pueden ser sometidos a la valoración del Grupo Europeo de Protección de Datos Personales para códigos aplicables a la zona euro o a las autoridades de control nacionales para aquellos que rigen en un territorio nacional. Sin embargo las problemáticas asociadas a los códigos son 3: representatividad, obligatoriedad y legalidad.(P.21 y 22 – [240])

El **agente de control interno** es un mecanismo que surge ante la proliferación de bases de datos privadas, con el fin de que no solo se controle el cumplimiento de las normas sino también se capacite, oriente e introduce a los ciudadanos en las novedades sobre tratamiento adecuado de datos personales en la empresa o entidad pública (P.23, último párrafo). Alemania lo introduce en 1977 como *comisario de protección de datos*, aplicable al sector privado. La directiva 95/46/CE lo renombra como *encargado del tratamiento*, nombrado por el responsable del

	<p>tratamiento para supervisar las operaciones con el fin de observar que no se “atentan contra derechos y libertades de los interesados”. Algunos distinguen si pertenece al sector público o al privado. La crítica a este mecanismo es la carencia de independencia efectiva al ser un empleado del responsable del tratamiento que determine si se realizó un tratamiento indebido.</p> <p>Un cuarto mecanismo es la autoridad de control creada por primera vez en la Ley del Land de Hesse sobre privacidad, siendo su naturaleza jurídica como una autoridad pública que informaba de los derechos a los titulares, asesoraba a los responsables del tratamiento, daba visto bueno a los códigos de conducta y fiscalizaba el cumplimiento de la ley(P.24) En todos los países hay una autoridad, en otros se divide la competencia; Inglaterra tiene el Registrador de Protección de Datos y el Tribunal Administrativo de protección de datos personales. La autoridad de control tiene los deberes de promoción, registro de las bases de datos, inspección, vigilancia, sanción, expedición de conceptos normativos, decreto de medidas cautelares.</p> <p>Sobre este mecanismo se fija una regulación de sus facultades, sus funciones (p.25-27), el nombramiento, la inhabilidad de estos, atribución de recursos de operación suficientes.</p> <p>Un quinto mecanismo son las tecnologías de protección de la intimidad que minimizan la recolección, empleo y uso ilícito de datos personales, “la Comisión de las Comunidades Europeas distingue tres tipos de productos: aquellos que respetan la intimidad, los que son diseñados cumpliendo la legislación; los que facilitan la protección de la intimidad; los que fomentan la protección de la intimidad, como los procedimientos de disociación de datos”(P.28) Se recomiendan prácticas de certificación y verificación independiente del cumplimiento de tales criterios en los productos.</p> <p>Un sexto mecanismo son los contratos – acuerdo entre los estados para facilitar la transferencia internacional de datos personales debido a la multiplicidad de normas que no lleva a un estándar de protección estable, en especial frente a terceros países como en el caso de los no-miembros de la Unión Europea. Es un ejemplo el acuerdo de <i>safe harbor</i> entre la UE y EUA. La problemática es que no reconoce como sujetos parte a los titulares de datos personales.</p> <p>Un séptimo mecanismo es el Defensor del Pueblo que dentro de sus facultades tiene la promoción y protección de los derechos humanos frente a entidades públicas.</p>
Análisis conceptual del documento	<p>El documento contempla la descripción de la evolución de la normativa sobre protección de datos europeos. Las generaciones de las leyes que fueron ampliando su ámbito de protección hasta la época actual, donde es importante el derecho fundamental del debido tratamiento de datos personales y los mecanismos para garantizar su respeto.</p> <p>La UE busca a través de sus directivas una uniformidad que permita seguridad jurídica en el</p>

	flujo interno de datos para que solo se preocupen de exigir esos mismos requisitos de facto a las transferencias internacionales de ciudadanos europeos.
Aportes del texto	<p>El análisis de los mecanismos existentes en el marco normativo europeo y la técnica legislativa que usan los países europeos del <i>omni bus</i> para promulgar leyes generales que no discriminan las circunstancias del procesamiento de datos.</p> <p>Los principios aplicables para el debido tratamiento de datos personales que se importan al ordenamiento jurídico colombiano desde la Unión Europea: licitud, calidad, lealtad, consentimiento informado, seguridad, confidencialidad, autorización y finalidad.</p>
Polémicas	¿El sistema de responsabilidad civil establecido en la directiva europea es objetivo o subjetivo?
Preguntas que suscita el texto	<p>¿Es posible consagrar un régimen de responsabilidad civil por indebido tratamiento de datos personales que incorpore la culpa y el dolo?</p> <p>¿Se protegen los derechos de las personas jurídicas a un adecuado tratamiento de los datos personales?</p> <p>¿Limita en exceso el principio del consentimiento en la cesión de datos las operaciones que hacen las empresas a diario?</p> <p>¿Podrían los códigos de conducta establecidos convertirse con el tiempo en una costumbre <i>praeter legem</i>?</p> <p>¿Satisfacen los mecanismos comentados los criterios de difusión, publicidad, asistencia, fiscalización y sanción que se presumen de la autoridad pública?</p>
Comentario Personal	Es importante resaltar que en el marco de la Unión Europea como antecedente se tiene la sentencia del tribunal constitucional alemán de 1983 sobre la ley del censo porque inicia el debate acerca del impacto de la tecnología en la personalidad del ser humano, la importancia de los mecanismos de protección y el control de su información personal.
Referencia de otros autores	<p>Nota 7(P.8) sobre el tema de derecho a la autodeterminación informativa o libertad informativa Frossini, Vittorio. Los derechos humanos en la era tecnológica. Anuario de Derechos Humanos, núm. 2, 1983. Recuperado el 03/04/16 de http://www.corteidh.or.cr/tablas/a19202.pdf.</p> <p>PARLAMENTO EUROPEO Y CONSEJO. Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.</p> <p>CONSEJO EUROPEO. Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).</p> <p>Saarenpää, Ahti. Europa y la protección de los datos personales. En Revista Chilena de Derecho Informático, núm. 3, 2003, pp.15-29</p> <p>TRIBUNAL CONSTITUCIONAL ESPAÑOL. Sentencia 254/1993(20 de julio). Recuperado el 03/04/16 de: http://hj.tribunalconstitucional.es/HJ/ES/Resolucion/Show/SENTENCIA/1993/254#complete_resolucion</p> <p>TRIBUNAL CONSTITUCIONAL ESPAÑOL. Sentencia 124 de 1998(13 de junio)</p> <p>TRIBUNAL CONSTITUCIONAL ESPAÑOL. Sentencia 11/1998(13 de enero)</p> <p>TRIBUNAL CONSTITUCIONAL ESPAÑOL. Sentencia 105/1998(18 de mayo)</p> <p>TRIBUNAL CONSTITUCIONAL ALEMÁN. Sentencia del 15 de Diciembre de 1983. Trad. Manuel Daranas. Publicado en BJC Boletín de Jurisprudencia Constitucional, 126-170, núm. 33, Enero de 1984. Madrid.</p>

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 04 de 23/02/2015
Propósito del diligenciamiento: Conocer los elementos y características del proceso de Habeas Data en los países de Latinoamérica para analizar el porqué de su naturaleza jurídica como proceso constitucional.	
Referencia Bibliográfica	Pérez Salazar, Gonzalo (2013) "Naturaleza Jurídica del Habeas Data", en Velandia Canosa, Eduardo Andrés (Dir. Cient.), Derecho Procesal Constitucional, Vol. IV, pp. 681-710. Bogotá: VC Editores y ACDPC.
Tema	Habeas data como garantía, acción, derecho fundamental o acción.
Conceptos	Procesal administrativo, procesal constitucional, derechos fundamentales.

Clave	
Idea principal	Exponer los argumentos por los cuales el Habeas Data es un proceso de naturaleza constitucional en Venezuela, en vez de ser un recurso, una garantía, un derecho fundamental.
Ideas secundarias relevantes	<p>Una primera tesis expone al Habeas Data como un derecho fundamental. El fundamento para tal tesis es el reconocimiento de la dignidad humana como eje central para configurar los derechos fundamentales, entre esos los llamado de tercera generación.(P.2)</p> <p>La doctrina que cita define el derecho a la protección de datos como: “(...)conjunto de normas y principios(...) establecidos a favor de las personas que pudieran verse afectados por el tratamiento de datos de carácter personal a ellos referidos”, estos incluyen: “autodeterminación informática, autodeterminación informativa, libertad informática, information control y habeas data” (P.3)</p> <p>En la jurisprudencia alemana inicial se desprendió el derecho la a autodeterminación de la información como derecho-instrumento que garantizaba, en cuanto al estar de por medio la tecnología de recolección, el derecho al libre desarrollo de la personalidad.</p> <p>El Tribunal Constitucional de Perú reconoció en sentencia del 7 de enero de 2011(Caso Margarita del Campo Vega) el derecho de acceso a la información, apoyándose en la Convención Americana de los DD.HH., art. 13 y también en la sentencia de la CIDH de Claude Reyes v. Chile. En principio lo limita a la entidad pública y concluye que es un desarrollo conceptual claro si se quiere la efectividad de la libertad de información.(P.3)</p> <p>En Ecuador se tiene como parte de la garantía constitucional del habeas data, para proteger la honra, la intimidad y la reputación. En España la posición es similar a la ecuatoriana, aunque lo concibe como un derecho de “control sobre los datos relacionados a la propia persona”.</p> <p>Las Constituciones de Guatemala (art.31), Nicaragua (art.26), Brasil (Art.5), Colombia (art.15), Paraguay(art.135), Perú (Art.200), Argentina(art.43), Venezuela (art.28) y Ecuador (art.92) consagran el derecho a la protección de datos junto a los derechos a la honra, la intimidad y el acceso a la información; en las constituciones de Brasil y Perú se reconoce el Habeas Data como una acción que garantiza los derechos que menciona y en cuanto a los derechos que contienen las constituciones de Paraguay, Perú y Colombia son más explícitas.</p> <p>La tesis central de los doctrinantes que conciben al habeas data como derecho fundamental (p.7) se debe a la posibilidad que le da a la persona de controlar y disponer de la información de él, aspectos que son enunciados como derechos en el artículo 28 de la Const. Venezolana. “Es un derecho del control de la información”.</p> <p>La tesis del Habeas Data como garantía parte de la instrumentalidad del mismo para garantizar otros derechos, que “busca proteger a los registrados del eventual perjuicio (...)” en el “(...) manejo inadecuado de aquella información” (p.8) Es decir ofrecer instrumentos para los derechos afectados por prácticas de almacenamiento y tratamiento, así como también la posibilidad de enterarse de la vulneración a estos.</p> <p>La tesis del Habeas Data como recurso se fundamenta en una visión holística de este, ampliando desde los derechos, el proceso y la acción hasta la petición inicial de acceso a la información.</p> <p>El habeas data es una subespecie del recurso de amparo.En Argentina, Colombia y Panamá se considera al Habeas Data un tipo de amparo constitucional. No así en Perú (trámite por el recurso de amparo), Honduras (por el mismo trámite que el Habeas Corpus), Brasil, Ecuador y Venezuela.</p>
Análisis	La tesis del habeas data como derecho fundamental confunde lo que permite el instrumento

conceptual del documento	procesal (habeas data) con el contenido de los derechos a debido tratamiento de la información, pues se busca efectivizar estos últimos por medio del primero. Además, al garantizar el derecho a la protección de datos personales se garantizan en algunos casos el derecho a la intimidad o a la información.
Aportes del texto	El derecho a la protección de datos se compone de los derechos de: Acceso, Rectificación, Cancelación.
Polémicas	¿Es el habeas data una acción, un proceso, una garantía o un derecho fundamental?
Preguntas que suscita el texto	¿Por qué debe ser considerado el habeas data como un derecho instrumental y al mismo tiempo un proceso constitucional?
Comentario Personal	NA
Referencia de otros autores	NA

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR :	GUIA N° 05 de 25/02/2015
Propósito del diligenciamiento: Comprender la clasificación y características del habeas data utilizada por el Profesor Oscar Puccinelli durante el análisis de los ordenamientos jurídicos de los países latinoamericanos.	
Referencia Bibliográfica	Puccinelli, O. (2004) Evolución histórica, análisis de las diversas especies, subespecies, tipos y subtipos de habeas data. Vniversitas, núm. 107, pp. 471-501, Pontificia Universidad Javeriana. Colombia, P.185-225.
Tema	Especies de Habeas Data en América Latina
Conceptos Clave	Habeas Data, Protección constitucional, derecho constitucional, protección de datos, tipos y subtipos.
Idea principal	“El autor del presente trabajo, plantea la necesidad de la protección jurídica frente al poder informático desarrollado desde el siglo XX.”(P.472)
Ideas secundarias relevantes	<p>La afectación de las libertades individuales por parte de las tecnologías automatizadas fue lo que motivó una preocupación por las consecuencias que tendrían en la esfera personal, la primera reacción jurídica fue el desarrollo del derecho a la intimidad o privacidad. El miedo al poder informático por su rápido desarrollo provocó su reacción jurídica: el derecho a la protección de datos personales junto a reglas para hacer frente a los peligros latentes (P.474)</p> <p>El derecho de la protección de datos se define como “aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho fundamental de la intimidad respecto del procesamiento manual o automático de datos” [HONDIUS, citado P.474]. Esta nueva rama del derecho protege los derechos que pueden ser lesionados por un tratamiento inadecuado de datos, que son bienes intangibles referentes a personas identificadas o identificables (Pérez Luño, citado P.475).</p> <p>Hay países que regularon con normas constitucionales el derecho a la protección de datos y otros que lo hicieron con normas legales. Con normas constitucionales Guatemala en el artículo 31 en 1985, Nicaragua en el artículo 26 en 1987, Brasil en 1988 agregándole un procedimiento especial llamado Habeas Data, es un caso particular este país debido a que el instituto se fijó como garantía de acceso a la información secreta o confidencial que tuvo la dictadura hasta 1985. Colombia lo reguló en el artículo 15 en 1991, así como leyes 510 de 1990, Paraguay hizo lo propio en el art. 26 un año después, Perú lo hace en 1993 consagrando además la acción de habeas data(art. 200 y 2°), Argentina lo incluye en 1994 en el art.43 y la ley 25326, Ecuador en 1996 en el art. 30 y la ley de Control Constitucional en art. 34 y 35, posteriormente en 1998 en el art. 200, Venezuela en 1999 con el articulo 27,28 y 281(que tiene tres novedades: habeas data impropio, habeas data colectivo y la garantía de confidencialidad a profesiones distintas</p>

del periodismo)

Otros países en la región han fijado normas legales para regular este derecho como México en el año 2000 con la reforma a la Ley de Protección al Consumidor (Capítulo VIIIbis sobre transacciones efectuadas a través de medio electrónico) y Chile en 1999 con la ley 19.628 sobre protección de la vida privada.

La clasificación que propone el autor no es taxativa y excluyente de otros rasgos o incompatible cada tipo con otro cuando se haga uso del habeas data, “por el contrario, pueden ser incoados dos o más de manera conjunta o sucesiva en cualquier proceso de Habeas data (v.gr., pretendiendo acceder formalmente a una información de la que ya se tomó conocimiento indirecto y, para el caso de coincidencia con lo así obtenido, formulando su cuestionamiento simultáneo —p. ej., exigiendo la rectificación de los datos, su confidencialización por tratarse de datos sensibles, y para el caso que esto último no fuera factible, su exclusión del registro”

Los dos criterios principales que tiene en cuenta para una clasificación inicial son: la legitimación por activa y la finalidad, en el primer caso si el peticionante o accionante es el directamente afectado y en el segundo criterio según lo que desea conseguir (acceso, bloqueo, exclusión, rectificación). Con base en lo anterior existe el habeas data propio para prevenir lesiones de derechos propios y el habeas data impropio para acceder a información pública o difundir información. (3 primeros párrafos p.488)

El tercer criterio es al momento de incoarse la acción y la tutela que persigue sobre sus derechos, lo que permite distinguir el habeas data preventivo si ocurrió antes de la lesión del derecho y habeas data correctivo cuando fue a raíz de esta lesión (pudo haber terminado o estarse consumando) y se pretende un resarcimiento.

Como cuarto criterio tenemos el radio de acción de los efectos habeas data interpartes o erga omnes y quinto criterio a la cantidad de legitimados habeas data individual y colectiva.

Haciendo una mezcla de los criterios de legitimación por activa, finalidad, tutela judicial que persigue se tienen habeas data propios reparadores y habeas data propios preventivos. Tienen los siguientes tipos:

Habeas data preventivos: Orientados a obtener información sobre el tratamiento de los datos o los datos que alojan de la persona, la finalidad del banco de datos, el tipo de información que recoge. Dentro de esta subespecie de habeas data se encuentra el habeas data informativo que consiste en conocer acerca de la recolección y tratamiento de datos, por ejemplo donde se realiza (localizador), quien lo hace, a partir de que fuentes se consiguen (autoral) que datos tienen (exhibicionista), para que lo realiza (finalista).

Habeas data reparadores: Para obtener modificaciones en el tratamiento del personal para evitar la lesión o para resarcir de esta cuando ocurra. Se encuentra el tipo aditivo: *actualizador* (datos que son ciertos el pasado), *aclarador* (situaciones ciertas que se interpretan inadecuadamente, se centra en las circunstancias que rodean al dato) o *inclusorio* (no se asentaron datos importantes para el interesado en el tratamiento de los datos); también el tipo *corrector*, que reemplaza los datos falsos por los ciertos o modifica datos que están incompletos (se centra en el dato, su fragmentación); habeas data exclusorio (de datos que no van conforme a la finalidad o que no se quieren actualizar o rectificar o no pueden ser objeto del tratamiento; reservador (para datos que deben tener unas políticas estrictas, autorizadas por los titulares de ellos y confidenciales de tratamiento); disociador (tener presente solo los rasgos o características sin vincularlos a una persona que pueda ser identificable); encriptador (es aquel que se pide para que cierto dato se transmite por medio de técnicas que ocultamiento, bloqueador (detener el tratamiento del dato mientras se surte la controversia, generalmente como medida cautelar); asegurador (exigir que se adecuen a las medidas técnicas para la seguridad de la base de datos); resarcitorio (tiene el fin de que las personas les sea reparado el

	daño moral y económico que sufrieron por el indebido tratamiento de sus datos personales).
Análisis conceptual del documento	<p>El documento presenta el fundamento para considerar la protección de dato personal como una rama independiente del derecho a la intimidad, así como también las diversas clases que sugiere el autor para clasificar las herramientas para protegerse de un tratamiento perjudicial o indebido de datos personales.</p> <p>La diversidad de pretensiones que pueden tomar resguardo en el derecho al habeas data hace posible que se consideren necesaria una clasificación doctrinal con el ánimo de agrupar la diversidad de intereses jurídicos semejantes y obtener una mejor argumentación cuando se articule con la acción procesal.</p> <p>El autor hace un corto recuento sobre el desarrollo del Habeas Data para centrarse en elaborar una clasificación de las clases que existen en América Latina a partir del análisis de sus constituciones y leyes.</p>
Aportes del texto	La clasificación didáctica que hace de los distintos tipos de habeas data es un acercamiento para deducir los derechos que protege cada tipo de habeas data y el grado de protección jurídica que puede tener de cada derecho como el tipo de habeas data que protege– para el caso de Colombia- cada uno de los mecanismos jurídicos.
Polémicas	¿Por qué la naturaleza instrumental del derecho a la protección de datos no permite afirmar que es en realidad una garantía en su moderna acepción?
Preguntas que suscita el texto	<p>¿Cuál es la diferencia entre derecho y garantía en la moderna acepción?</p> <p>¿La acción de tutela en sus efectos inter comunis e inter pares es un mecanismo de habeas data colectivo para Colombia o debe crearse uno específico? ¿Cómo afecta esto a la estructura conceptual de las acciones de grupo?</p> <p>¿Es la acción de grupo un mecanismo de habeas data colectiva?</p>
Comentario Personal	Este artículo ha presentado un esquema general de la manera como los países latinoamericanos regulan la protección de datos personales de sus ciudadanos. En mayor medida tienen una estructura común y adicionan aspectos específicos como procedimientos especiales y tipologías de datos personales.
Referencia de otros autores	<p>Eguiguren P., Francisco J.; (1997). 5. EL HÁBEAS DATA Y SU DESARROLLO EN EL PERÚ. <i>Ius et Praxis. Recuperado el 16/04/2016 en: http://www.redalyc.org/articulo.oa?id=19730111</i></p> <p>ZÚÑIGA URBINA, FRANCISCO, El derecho a la intimidad y sus paradigmas, “Ius et praxis”, publicación de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca (Chile), 1997, año 3, n° 1, “Derecho a la autodeterminación informativa y acción de Habeas data en Iberoamérica”, págs. 300/1.</p>

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR :	Camilo José Puello Rincón
	GUIA N°06 de 04/03/2015
Conocer el análisis realizado por Nelson Remolina sobre el grado de protección jurídica que ofrecía la ley 1266 de 2008 en Colombia, a partir de una comparación con la directiva europea 95/46/CE.	
Referencia Bibliográfica	Remolina-Angarita, N. (Enero-Junio, 2010a). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? <i>International Law</i> , N°16.489-524. Recuperado el 19 de abril de 2016 de: < http://www.redalyc.org/articulo.oa?id=82420041015 >
Tema	Protección de datos personales y el nivel de adecuación normativa adecuado para garantizar su protección.
Conceptos Clave	Habeas data, nivel adecuado, estándar europeo, datos personales, transferencia internacional de información.
Idea principal	Los datos personales son una clase de información que aumentó su importancia social y económica en el siglo XXI por la utilidad que generan para las empresas o instituciones

	gubernamentales. Todo se debió a la revolución de las TIC que aceleraron el proceso de tratamiento y transferencia internacional de datos personales. Por lo anterior se expidieron normas jurídicas para regular esa actividad.
Ideas secundarias relevantes	<p>Las características de los sistemas de información público y privado son comunes: “i) se nutren de datos personales, ii) ofrecen innumerables posibilidades para recolectar, almacenar y circular esa información en poco tiempo y de manera imperceptible para las personas a que se refieren los datos, iii) No son absolutamente seguros, iv) evolucionan rápidamente, v) traspasan las fronteras físicas”(P.492)</p> <p>Las TIC han sido las impulsoras del tratamiento, globalización y transferencia internacional de datos personales. Hay reglas para garantizar la protección en todos los procesos, Europa ha sido un continente pionero al fijar reglas jurídicas.</p> <p>La Unión Europea ha sido entidad pionera en regular de forma jurídica el tratamiento de datos personales, exigiendo su cumplimiento para tener el nivel adecuado de protección(P.493) Las consecuencias de contar con un nivel adecuado de protección son principalmente económicas, aunque no se descartan subjetivas de percepción de seguridad. Colombia no cuenta con el nivel de protección requerido.</p> <p>Existen requisitos legales para que un país sea considerado con un nivel adecuado de protección de datos personales. Esas reglas buscan evitar paraísos informáticos o <i>data havens</i>. El artículo se refiere sólo a la transferencia internacional de datos personales y no a la recolección internacional de datos personales (caso de empresas de Google y Facebook)</p> <p>La nota 18 del artículo establece un recuento histórico de las leyes que surgieron entre 1970 a 1980 en el mundo sobre habeas data. Entre esos destaca la <i>Fair Reporting Act</i> de 1970 para proteger a los clientes de los establecimientos de crédito., la <i>Privacy Act</i> de 1974 en Estados Unidos.</p> <p>Las reglas relativas a la transferencia internacional de datos personales, válidas a nivel internacional se crearon para evitar que se desvanezcan los esfuerzos nacionales de protección al exportar los datos. Esto se conoce como “Principio de continuidad de la protección de datos” y significa una garantía que obliga al transferir datos entre países a“(…) verificar que el país importador garantice un nivel “<i>adecuado</i>” de protección de datos personales. En este sentido, la expresión “<i>adecuado</i>” se refiere a que el Estado importador tenga un grado de protección superior, igual, similar o equivalente al del Estado exportador”(P.497)</p> <p>La resolución 45 de 1995 estableció el requisito para el flujo entre dos países: tener un nivel de protección jurídica semejante. Según Remolina no se conocen criterios en el documento para identificar que se tienen <i>garantías comparables</i>. En la Unión Europea la situación fue de prohibición en la transferencia de datos, cuando el país externo no tuviese los mismos niveles de protección que el país emisor de la transferencia de datos. En la Directiva 95/46/CE europea se cambio la posición, se permite la transferencia si garantiza <i>nivel de protección adecuado</i>. Es necesario saber que se entiende por nivel adecuado.</p> <p>Los factores para entender que es el nivel de protección adecuado son de índole regulatoria e instrumental que Remolina fija a partir del análisis de los artículos que emite el grupo del artículo 29 de protección de datos personales de la Unión Europea (P.500). El primero se compone de los derechos del titular del dato y de los deberes del encargado o responsable del tratamiento, (P.500) explícitos que comprende el habeas data y el segundo son los mecanismos establecidos para su efectividad: judiciales o no judiciales, especialmente una autoridad pública de control.</p> <p>El análisis para establecer el nivel de protección adecuado a nivel concreto son a) el contenido de las normas aplicables y b) los medios para garantizar su efectiva aplicación.(P.499 y 500)</p>

“No todos los países tienen una protección uniforme” (p.500) Existen una serie de principios comunes entre las normativas europeas, internacionales y locales que el grupo del artículo 29 extractó: limitación de la finalidad, calidad de los datos y proporcionalidad, transparencia, seguridad, acceso, rectificación y oposición, restricciones a las transferencias sucesivas a terceros países. Además de aspectos sobre datos sensibles y tratamiento automatizado.

Los países aprobados por la Unión Europea como lugares con niveles adecuados han hecho lo siguiente: promulgar normas generales que contienen los principios básicos, tienen disposiciones sectoriales, adquieren compromisos internacionales y normas constitucionales (aunque este criterio no es tan decisivo al verse la tabla que los aprobados no tienen normas constitucionales.) (P.501 y P.502) (Ver Tabla 2 Cuadro comparativo de aspectos que han tenido incidencia en los procesos de “nivel adecuado” de terceros países frente a la Comisión Europea.)

“Obtener el nivel de adecuación hace más competitivos a los países en la medida en que tienen luz verde para recibir datos provenientes de Europa, lo cual es un factor cardinal para el desarrollo de varios negocios.” (P.503)

“Así las cosas, resulta importante establecer si Colombia puede considerarse como un país que proporciona un nivel de protección adecuado en el sentido del artículo 25 de la Directiva 95/46/CE”. Es una ley sectorial la 1266 de 2008, por ello se aplica la sentencia T-414 de 1992 (esto teniendo en cuenta que está vigente la ley 1561 de 2012 regulación integral del *habeas data* y que no tiene en cuenta el artículo 15 constitucional).

El marco normativo de la protección de datos personales en Colombia está a la cabeza del artículo 15 de la Constitución de 1991 junto a más de 60 normas expedidas desde 1951 que tocan tangencialmente aspectos de los datos personales. “De las normas analizadas no se deriva una tipología temática o estructural común a todas ellas. Reinan la variedad de clases de información y la creación de muchos sistemas de información, registros y bases de datos al servicio del Estado y de los particulares” (P.505) Adicionalmente existen más de 150 sentencias que han desarrollado la línea jurisprudencial tomando como extremos la T-414 de 1992 y la T-421 de 2009, “(...) en las cuales ha definido el alcance y características del *habeas data* así como las condiciones que deben rodear el tratamiento de los datos personales” (P.509).

La ley 1266 es una regulación parcial y sectorial del derecho de *habeas data*, menciona la corte en la sentencia C-1011 de 2008. Los conceptos proferidos por la Superintendencia Financiera (Concepto 2009029082-002 de 4 de Junio de 2009) y la Superintendencia de Industria y Comercio (09037876 del 12 de junio de 2009) afirmaron que dicha ley es parcial por ser aplicable a la información financiera, crediticia, comercial, de servicios y la que proviene de terceros países. “No es una norma que regule el núcleo esencial del derecho fundamental en estudio para toda clase de información personal, sino una disposición que reguló en forma exhaustiva y casuística algunos elementos del citado derecho respecto de la información sobre el cumplimiento e incumplimiento de obligaciones dinerarias” (P.512)

Sobre la ley 1266 de 2008 se analizarán las cuestiones de: (...) (1) Datos sensibles. (2) Derecho de oposición. (3) Decisiones individuales automatizadas y (4) Transferencia internacional de datos personales.” (P.512)

El fundamento jurídico constitucional de los mecanismos para la protección de los datos personales es el derecho de oposición. Remolina comenta tres situaciones en las que es procedente y necesario este: 1) Cuando no es necesario el consentimiento previo del titular del dato para realizar el tratamiento, pero la situación surgida en la persona titular lo motiva, 2) Cuando las bases de datos tienen por finalidad la publicidad comercial, 3) Cuando las decisiones con respecto al titular del dato se toman con base en decisiones surgidas a partir de tratamiento

	<p>automatizado.</p> <p>Definir si un banco de datos extranjero tiene nivel de protección depende de los responsables del tratamiento</p>
Análisis conceptual del documento	El documento es un bosquejo inicial acerca del nivel de protección que ofrece la norma ley 1266 de 2008 a los datos personales y su recolección, almacenamiento y tratamiento de la información personal. Aún queda pendiente el análisis del nivel de protección que tienen los mecanismos para garantizar el derecho de la protección de datos personales.
Aportes del texto	El documento permite identificar el marco normativo sustancial colombiano que ha regulado de manera fragmentada la protección de datos personales.
Polémicas	NA
Preguntas que suscita el texto	¿Cómo hará Colombia para obtener el nivel de protección adecuada por parte de la UE?
Comentario Personal	Este documento permite ser el disparo inicial para indagar sobre el problema de investigación planteado por el profesor Nelson Remolina acerca del nivel de protección de los mecanismos que tiene el ordenamiento jurídico, debido a que su artículo se centra en los aspectos sustanciales de la regulación y a que hasta el momento de elaboración de esta ficha y en el momento presente, no se han encontrado estudios iniciados por él al respecto.
Referencia de otros autores	<p>Blanco, María José. Globalización de la privacidad: hacia unos estándares comunes – transferencias internacionales de datos, VI Encuentro Iberoamericano de Protección de datos, Cartagena, 2008.</p> <p>Garriga-Domínguez, Ana. Tratamiento de datos personales y derechos fundamentales. (Dykinson, Madrid: 2004).</p> <p>Kuneva, Meglena. Roundtable: Keynote speech , Citado por Katitza Rodríguez-Pereda. Ponencia presentada en el I Seminario Euro-Iberoamericano de protección de datos: La protección de los menores, Cartagena, 2009.</p> <p>Remolina-Angarita, Data protection: Riesgos y desarrollo (Énfasis en el caso colombiano),328 Revista de la Academia Colombiana de Jurisprudencia, 1, 35-68 (2005).</p> <p>Rodotà, S. (2011). Democracia y protección de datos. Cuadernos De Derecho Público, (19-20). Recuperado de http://revistasonline.inap.es/index.php?journal=CDP&page=article&op=view&path%5B%5D=690</p> <p>Schwartz, Paul. Property, privacy and personal data, 117 Harvard Law Review, 7, 2055-2128(2004)</p> <p>Yves Poullet & Jean-Marc Dinant, Hacia nuevos principios de protección de datos en un nuevo entorno TIC, 5 Revista Internet, Derecho y Política, IDP, 35 (2007). Recuperado el 24/04/16 de: http://www.uoc.edu/idp/5/dt/esp/poullet_dinant.html</p> <p>Normas extranjeras e internacionales</p> <p>ONU. Resolución 45/95 del 14 de diciembre 1990, “principios rectores para la reglamentación de los ficheros computarizados de datos personales”.</p> <p>Consejo de Europa. Convenio 108 del 28 de Enero de 1981</p> <p>Parlamento europeo y Consejo de Europa. Directiva 95/46/CE del 24 de octubre de 1995</p>

	<p>Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, <i>Primeras orientaciones sobre la transferencia de datos personales a países terceros: posibles formas de evaluar la adecuación</i> (Bruselas, 1997).</p> <p>Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, <i>Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE</i> (Bruselas, 1998).</p> <p>Normas y jurisprudencia colombianas</p> <p>Corte Constitucional colombiana. Auto 159 del 21 de Abril de 2009. Corte Constitucional colombiana. Sentencia T-307/1999 Corte Constitucional colombiana. Sentencia C-1011 de 2008.</p> <p>Decreto 2591 de 1991(habeas data); datos personales: Decreto 4759 de 2005, Decreto 1151 de 2008; información especial huella dactilar (decreto 2628 de 1951, resolución 160 de 1996 Registraduría), historia clínica(ley 23 de 1981, decreto 2280 de 1991, ley 320 de 1996, decreto 1543 de 1997, resolución 1448 de 2006 del Ministerio de Protección Social), censos de población(ley 79 de 1993 y decreto 1100 de 2005), seguridad social(ley 488 de 1998, decreto 1406 de 2009, ley 633 de 2000, decreto 889 de 2001, ley 1122 de 2007), el dato comercial y financiero(circular 23 de 2004 de la SuperBancaria(Superfinanciera), ley 986 de 2005, Resolución 1732 de la Comisión de Regulación de Telecomunicaciones(hoy Comisión de Regulación de Comunicaciones), ley 1380 de 2010), antecedentes penales(ley 906 de 2004), datos de menores(ley1098 de 2006), de personas con discapacidad(ley 1306 de 2009 y 1346 de2009)</p> <p>Algunos datos personales son tratados como reservada(ley 96 de 1985, decreto 2241 de 1986, ley 73 de 1993, ley 412 de 1997, decreto 889 de 2001, decreto 1100 de 2005, ley 985 de 2005, decreto 4816 de 2008, ley 1288 de 2009, ley 1306 de 2009) y con medidas especiales para su protección y fines(ley 200 de 1995, ley 734 de 2002, decreto 3680 de 2009)</p> <p>Otras normas se enfocan en la confidencialidad, seguridad y privacidad de los datos (ley 270 de 1996 y ley 527 de 1999, decreto 1747 de 2000, Resolución 1732 de 2007 de la CRT, ley 1328 de 2009)</p> <p>Hay normas sobre circulación de datos entre entidades (ley 962 de 2005, ley 1122 de 2007, ley 1176 de 2007, decreto 4816 de 2008), limitan el uso (decreto 4816 de 2008, decreto 3680 de 2009), para ámbitos específicos (publicidad la resolución 1732 de la CRT.</p> <p>Hay una ley que consagra conductas punibles (ley 1273 de 2009)</p> <p>Otras normas se refieren a las bases de datos especiales: personas vinculadas al estado(ley 13 de 1984, ley 190 de 1995, ley 489 de 1998, decreto 1049 de 2001), personas infractoras(ley 53 de 1989, ley 769 de 2002, ley 1270 de 2009), beneficiarios de servicios estatales(ley 789 de 2002, ley 1251 de 2008, ley 1276 de 2009, ley 1286 de 2009), del gasto social(ley 1176 de 2007, decreto 4816 de 2008, ley 1276 de 2009) sistemas de información sobre delitos(ley 679 de 2001, ley 1336 de 2009), contratación estatal(ley 598 de 2000) registro de adquirentes de pólizas de seguros(ley 1328 de 2009,art.78-79 y decreto 3680 de 2009)</p> <p>Otras normas dan permisos especiales para acceder a bases de datos con fines de investigación penal (ley 906 de 2004), combatir lavado de activos(ley 526 de 1999, ley 1121 de 2006), la trata de personas(ley 985 de 2005) o defender la seguridad nacional(decreto 643 de 2004) y facilitar la inteligencia(ley 1288 de 2009)</p>
--	---

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 07 de 03/05/2015
Propósito del diligenciamiento: Comprender el concepto de datos personales en el modelo europeo de protección de datos personales a partir del análisis de la postura oficial acerca de los elementos que integran el concepto de dato personal.	
Referencia Bibliográfica	Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales (CE, 2007), <i>Dictamen 4/2007 sobre el concepto de datos personales</i> . Bruselas. Consultado el 29/04/16 de: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf
Tema	Concepto de dato personal en la directiva 95/46/CE
Conceptos Clave	Principios generales, Derecho, respuesta definitiva, <i>quid juris</i> , analogía, inducción, abstracción, homogeneidad del sistema, conexión lógica
Idea principal	“El objetivo del presente Dictamen del Grupo de trabajo es alcanzar un acuerdo sobre el concepto de datos personales, los casos en que debe aplicarse la legislación nacional sobre protección de datos y la manera en que ésta debe aplicarse.”
Ideas secundarias relevantes	<p>“Alcanzar una definición común del concepto de datos personales equivale a definir lo que entra o queda fuera del ámbito de aplicación de las normas sobre protección de datos.”</p> <p>“La directiva maneja un concepto lato de datos personales (...) El ámbito de aplicación de la Directiva excluye varias actividades y la flexibilidad impregna el texto con el fin de proporcionar una respuesta legal apropiada a las circunstancias imperantes en cada caso” (p.4) y su objetivo es proteger las personas físicas.</p> <p>“La mejor opción es no restringir indebidamente la interpretación de la definición de datos personales, sino tener en cuenta que existe una considerable flexibilidad en la aplicación de las normas a los datos. “(P.4)</p> <p>Los componentes principales de la definición europea de dato personal son: “toda información”, “sobre”, “persona física”, “identificada o identificable”.</p> <p>“Toda información” hace referencia amplia a aquel conjunto de hechos objetivos, actividades, pensamientos de una persona y los juicios de valor social emitidos por el entorno que le rodea, que posteriormente son almacenados en medios mecánicos o digitales (criterios de formato, contenido y naturaleza de la información). En resumen es toda la información que pueda decir algo de una persona o hacernos formar una idea determinada de ella.</p> <p>“Sobre” hace referencia a quien pertenece la información, si es una persona natural o jurídica y bajo qué relación se recogen esos datos. En resumen es la manera como puede asociarse la información como perteneciente a una persona, “siguiendo la misma línea de razonamiento, podría afirmarse que para considerar que los datos versan «sobre» una persona debe haber un elemento «contenido» o un elemento «finalidad» o un elemento «resultado». (P12) Estos elementos deben considerarse como condiciones alternativas y no acumulativas.</p> <p>“Del análisis anterior se desprende que a la pregunta de si los datos se refieren a determinada persona hay que contestar, analizando cada dato, en función de sus características.”(P.13)</p> <p>“Persona física”</p> <p>“Identificada o identificable” hace referencia a que la información referida a una persona a través de los criterios mencionados puede efectivamente habilitarnos para distinguirlo de otro que tenga rasgos semejantes o ejecute una actividad similar. “La identificación se logra normalmente a través de datos concretos que podemos llamar «identificadores» y que tienen una relación privilegiada y muy cercana con una determinada persona” (P.13) También implica que pueden usarse con medios, que se creen en el futuro, para hacer identificable una persona a partir de datos que estaban anónimos debido a la ausencia de circunstancias técnicas idóneas para usarlos. “Y, sin embargo, el tratamiento de esa información sólo cobraba sentido si permitía la identificación de individuos concretos y su tratamiento de una manera determinada.”(P.17)</p>

	<p>Como medida técnica para ocultar la identidad o difuminarla tenemos <i>la seudonimización, el enciframiento, la anonimización.</i></p> <p>La utilización de seudónimos permite recopilar bastante información acerca de una persona, sin que en conjunto pueda identificarse rápidamente; es un procedimiento por medio del cual se selecciona aleatoriamente un “nombre falso”. Un buen ejemplo lo constituyen la forma de navegación privada que se encuentran en varios navegadores web que evitan asociar el historial de navegación por sitios web con una dirección IP específica o con los hábitos de navegación previamente almacenados acerca de ese dispositivo.</p> <p>El enciframiento es un procedimiento por medio del cual se convierten los datos en un código determinado y una clave para acceder a los datos, sin esa clave es imposible acceder a la identidad real y determinar a quién pertenecen los datos. La anominización consiste en separar de la información los datos que puedan identificar a una persona específica, de esta manera ya no es posible realizar un análisis de pertenencia a esa persona.</p> <p>Los datos de personas fallecidas son personales en tanto indiquen algún rasgo o permitan emitir un juicio sobre otra persona con la cual tiene parentesco.</p>
Análisis conceptual del documento	El énfasis en la definición uniforme de dato personal para toda la Unión Europea se centra en los cuatro elementos estructurales: <i>toda información, sobre, persona física, identificada o identificable.</i> A partir de estos elementos la Comisión Europea considera que pueden establecerse claramente los datos personales, por esta razón entra a hacer una descripción enunciativa de lo que debe entenderse al mencionar cada elemento y deja la tarea de colmar plenamente los rasgos a la legislación nacional de cada país.
Aportes del texto	El análisis estructural del concepto de datos personales en el modelo europeo de protección de datos personales.
Polémicas	La polémica sobre la protección de los embriones congelados a través de la figura del que está por nacer que se le otorgan derechos, menciona el caso de la herencia, donde a algunos se les reconoce personalidad jurídica.
Preguntas que suscita el texto	¿Pueden ser protegidos los datos personales de una compañía, en relación a su buen nombre y al uso de los datos personales que maneja no relacionados estrictamente con un fin económico o de explotación?
Comentario Personal	Este artículo ha permitido comprender como se aplica la noción de dato personal a las actividades de tratamiento de información para identificar cuáles son de datos personales y debe aplicarse la directiva y cuales no lo son.
Referencia de otros autores	NA

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 08 de 17/06/2015
Propósito del diligenciamiento: Conocer el desarrollo doctrinario y jurisprudencial, incipiente en Colombia, del habeas data hasta el momento de la elaboración de este importante trabajo que es el año de 1994; se destaca la importante mención de derechos conexos que es importante tener en cuenta.	
Referencia Bibliográfica	Remolina-Angarita, N. (Noviembre, 1994). El habeas data en Colombia. Revista de Derecho Privado, núm.15. Facultad de Derecho de la Universidad de los Andes. Recuperado en 09 de abril de 2015, de https://derechoprivado.uniandes.edu.co/components/com_revista/archivos/derechoprivado/pri319.pdf

Tema	El desarrollo jurídico del Habeas Data y su protección en Colombia.
Conceptos Clave	Derechos conexos al habeas data, propiedad del dato personal, poder informático, derecho a la intimidad
Idea principal	Exponer el desarrollo de este derecho fundamental en Colombia a partir de las discusiones jurisprudenciales, académicas y normativas que se han dado.
Ideas secundarias relevantes	<p>La Constitución de 1991 incluyó derechos que protege a través de múltiples mecanismos. De ellos destaca el derecho a la intimidad, dentro del que se incluye la protección frente a la tecnología de la información y la comunicación que pueda vulnerar el derecho fundamental.</p> <p>La doctrina española e italiana tiene una gran experiencia en los mecanismos de protección de las personas frente a los eventuales abusos del poder informático.</p> <p>El artículo 15 de la Constitución colombiana señala que las personas tienen el derecho de conocer, rectificar, actualizar las informaciones que se hayan recogido sobre ellas por cualquier persona privada o pública. “Lo anterior implica que los interesados- cuyos datos son objeto de un tratamiento automatizado- no sean privados del control sobre los datos que les concierne”(P.191)</p> <p>Sin embargo el autor afirma que hay otros sentidos para el habeas data, “(...) es un mecanismo o garantía esencial para afianzar la protección efectiva de otros derechos fundamentales, verbigracia, intimidad, buen nombre, etc.”(P.193)</p> <p>El habeas data es “mecanismo esencial para afianzar la protección efectiva de otros derechos fundamentales (...)” “(...) posee la virtud de restituir, proteger y evitar que se prolongue la indebida intromisión en la intimidad o en otros derechos fundamentales (...) otorga la posibilidad de impedir el uso de datos por parte de terceras personas (...)”(P. 193 y 194). Las entidades que recogen la información están obligadas a darla a conocer, actualizar o corregir a sus titulares la información cuando recolecten nuevos datos que les concierne.</p> <p>En Alemania y España se le denomina derecho a la autodeterminación informativa.</p> <p>“Aunque algunos derechos fundamentales no aparezcan expresa o directamente vulnerados por la acción u omisión de un particular o del Estado, sin embargo, su conexión con otros derechos fundamentales es de tal naturaleza que, sin la debida protección de aquellos, estos prácticamente desaparecerían o harían imposible su eficaz protección.” (p.195)</p> <p>“Lo importante es que las personas no pierden el control de su propia información, así como de su uso” (P.194). Algunos aspectos como la finalidad, el alcance del permiso y por último el consecuente abuso al superarse este.</p> <p>1.2 Derechos conexos</p> <p>El derecho a la información es afectado en la medida que se divulguen o conserven datos que no son ciertos o que son erróneos actualmente, lo cual permite ejercer un derecho de rectificación para que se informe más ajustada a la realidad. El Habeas Data ayuda a que se publique solo información veraz, pero se diferencia en el momento que se puede ejercer y contra quienes, en el primer caso en cualquier momento (antelación o posterioridad a la publicación o uso) y en lo segundo ante los bancos de datos y archivos. El derecho a la rectificación es una derivación del Habeas Data.</p> <p>La honra y el honor se ven vulnerados cuando la información desestima el valor social de la persona y el valor propio que tiene de ella. Hay un derecho que está íntimamente vinculado con estos que es el buen nombre e imagen, que se vulnera cuando se genera una imagen que resta reconocimiento o nos da una apariencia errada a otros; respecto al habeas data hace parte del Habeas Data rectificatorio o cancelatorio.</p>

Por último el derecho a la igualdad es vulnerado cuando se le realiza un tratamiento a los datos de alguien diferente al que haría el responsable a otros que se hallan en la misma situación sin una finalidad clara o justificable para ello. Esto aplica cuando se incumplan las políticas de tratamiento frente a la persona.

Un derecho que es vulnerado en conexidad con el habeas data, y que se resalta dada la cercanía, es el de intimidad, este derecho puede referirse **en términos amplios** como derecho a proteger la vida privada y familiar o **en términos estrictos** como derecho para proteger de las lesiones, en este caso sería con miras a detener y resarcir de los daños causados.

Las nuevas tecnologías que han surgido con la computación facilitan una mayor captura de datos de las personas (poder informático), y ponen al individuo como objeto de decisiones o conductas privadas o públicas que pueden afectarle, es un nuevo dominio social; hay una nueva faceta surgiendo del derecho a la intimidad que no niega la intromisión en la vida privada de la sociedad y da una facultad jurídica a las personas para controlar el uso de los datos acerca de cada uno. Las violaciones producidas son de dos tipos: i) acceso inadecuado o sin permiso a la información de la persona o a su esfera personal ii) Abuso del permiso otorgado.

La protección jurídica frente a esas violaciones comienza con el desarrollo conceptual de la libertad informática en la Ley de protección de datos personales del Land de Hesse del 7 de octubre de 1970, luego en 1973 la ley sueca, en 1974 la Privacy Act de USA. A nivel constitucional se incluye en Portugal (art.35 en 1977), España (art.18 en 1978).

La sentencia T.-414 de 1992 analiza la situación, en ese momento, de la protección de datos personales en Colombia. Normativamente hay reglas sectoriales en campos como imagen, domicilio, correspondencia, comunicaciones, reserva documental, secreto profesional, reserva tributaria, reserva bancaria, reserva sumarial, reserva comercial, secreto industrial, reserva estadística(202)

El origen en Colombia han sido las violaciones en el marco de la relación crediticia con las instituciones bancarias que publican sin autorización o mantienen un dato que es inexacto o que no quieren corregir, frente a lo cual se instaura acción de tutela cuyos resultados tuvieron diversas interpretaciones sobre el alcance, naturaleza y efectos del habeas data.

La sentencia T-414 de 1992 establece algunas definiciones y aspectos que en ese momento generan controversia:

- Propiedad del dato personal está en cabeza de quien lo proporciona, por ello quien encuentra información que esté relacionada con un individuo y posteriormente la almacena, debe solicitar la autorización e informarle del tratamiento (fines y condiciones) que harán si no media una relación contractual, evitando aclaraciones en el difícil punto de análisis cuando hay un contrato de adhesión y las responsabilidades por un tratamiento indiscriminado con que “el simple requisito de que la actora haya autorizado la inclusión de sus datos en el banco de datos, es suficiente para que el administrador del banco de datos determine sin fundamento alguno que hacer o no con ellos, y la peticionaria por haber dado la autorización pierde el control sobre los mismos”(P.204)
- Vigencia del dato personal queda en cabeza del responsable del tratamiento de datos personales, pues estos son por naturaleza mutables, a fin de evitar que se circulen perfiles virtuales falsos o inmutables de una persona, eliminando su oportunidad de mejorarlo o actualizarlo, situación que vulnera el derecho al buen nombre y a la honra. Aquí hay situaciones polémicas como el derecho al olvido, la prescripción de una obligación como cancelación de un dato, que es cancelación y que es actualización, como se justifica la existencia de archivos históricos y por último el **límite temporal de los datos**, esta última cuestión que afectaría gravemente a la persona si se permite una prolongación indefinida de la información almacenada sin modificaciones.(204-

	<p>205)</p> <p>Como consecuencia del límite temporal debe declararse la <i>prescripción</i> del dato personal por medio de tutela(claridad que es de esta porque para la obligación hay una vía adecuada) o en conexidad con la sentencia que declara prescrita una obligación</p> <ul style="list-style-type: none"> • Derecho al olvido se presentan cuando desaparecen las causas que dieron origen o fines para tratar el dato personal. En el caso de la sentencia T-022 de 1993 se declara que la vigencia limitada del dato personal (debido al cumplimiento de la causa o condición que generó su recolección) per se lleva a que se cancele el mismo en el respectiva registro de datos, ya que es exigencia de actualización y de dignidad humana. En casos particulares de obligaciones la prescripción de esta automáticamente conlleva la del dato personal relacionado (sentencia T-486 de 1992), aunque se modifica por la SU-528 de 1993 al exigir que previamente un juez haya declarado la prescripción de la obligación porque el juez de tutela solo se pronuncia en la violación de derecho al habeas data. Frente a esta sentencia hubo dos posiciones discrepantes en las que se argumentaba que la declaración era sobre la caducidad del dato por no ser actual y que la prescripción legal es un indicador para establecerlo, por ello la tutela es un instrumento transitorio de protección conciliando efectividad de los derechos fundamentales y exigencia de seguridad jurídica. Esto nos lleva a la actualización, que la Corte la define como el cumplimiento de unos presupuestos para cambiar el dato de de la persona al que refleje la situación actual y eliminar el anterior, de cara a la idea que puedan hacerse otros (Sentencia T-157 Y T-164 de 1994) y no solo importa el criterio de veracidad; está prohibido el uso de bases de datos históricas, esto es de información desactualizada que queda guardada o trasladada a otro sitio, pudiendo perjudicar el buen nombre de la persona a futuro si es filtrada la información con voluntad o sin intención. • Prevalencia del derecho a la intimidad, al buen nombre y a la honra frente al derecho a la información. (Sentencia T-414 de 1992) porque se encuentra inmerso en la personalidad como elemento esencial que se relaciona con la dignidad humana. Aquí la Corte hace una interpretación conjunta del artículo 15 y del 20 Superior. • Procedencia del habeas data para solicitar la historia clínica por referirse a información personal e individual y no a documentos públicos, que abre las puertas a que otros puedan considerarse legitimados para acceder la información (Sentencia T-158 de 1994). <p>La Sentencia C-008 de 1995 declara inexecutable el proyecto de ley presentado en ese momento por vicios de forma, aunque para Remolina no cumple con los requisitos porque no establece una autoridad pública que garantice los derechos, hay un concepto amplio de información comercial (toda información relevante para tomar decisiones), hay poca precisión sobre la información que es personal, sobre la cancelación del dato hay términos excesivos en materia comercial, “la persona que incumpla una obligación comercial o que la realice pero de manera “irregular” debe ser sancionada de la manera más ejemplar y severa que el delincuente penal”, responsabilidad civil por daños causados (P.217-219)</p> <p>Conclusión N°3: “El habeas data, surge en nuestra constitución, como un derecho fundamental y mecanismo jurídico efectivo para garantizar la protección de la intimidad, buen nombre, y demás derechos conexos frente al proceso de creciente informatización de las relaciones sociales, a través de banco de datos”(P.220)</p> <p>Conclusión N°8: “El único titular del dato personal es la persona a que concierne (...)” y se generan las siguientes consecuencias (P.221-222):</p> <p>“a) La persona es la única legitimada para permitir la divulgación de datos concernientes a su vida privada. Ella debe autorizar su inclusión en bancos de datos y conocer los fines por los cuales se incorporan y permanentemente puede controlar el uso de los mismos</p> <p>b) Como consecuencia de lo anterior, la persona puede impedir que sus datos” se usen sin su consentimiento</p> <p>d) Los datos deben usarse con un fin necesario y legal, que sean actuales y adecuados al fin que se pretende y haya medidas preventivas.</p>
--	--

Análisis conceptual del documento	Este documento analiza las características, derechos y alcances del habeas data desde la doctrina y su aplicación en Colombia a través de la jurisprudencia.
Aportes del texto	Como se ha gestado el desarrollo teórico del derecho al habeas data a partir de la jurisprudencia original proferida por el tribunal supremo de lo constitucional en Colombia, que ha seguido la tendencia de protegerlos como derechos fundamentales presentada en otros países. De manera destacada expone que se relaciona con otros derechos como el buen nombre, la honra, el honor.
Polémicas	No se encuentra alguna polémica
Preguntas que suscita el texto	No generó pregunta alguna
Comentario Personal	Permitió comprender los orígenes en Colombia del derecho al habeas data
Referencia de otros autores	ONU. Comisión de derechos Humanos. Documento E/CN4/116 de 1973. Donde se indicant a manera ilustrativa los atentados contra la intimidad. Colombia. Consejo de Estado. Expediente AC-543 de marzo 3 de 1993. Consejero Ponente Juan de Dios Montes Hernández. Colombia. Corte Constitucional. Sentencia T-022 de 1993. Colombia. Corte Constitucional. Sentencia T-486 de 1992.

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : CAMILO JOSÉ PUELLO RINCÓN	GUIA N°09 de 18/03/2016
Propósito del diligenciamiento: Comprender la formulación teórica que se realizó en el derecho norteamericano acerca del derecho a la intimidad o privacidad.	
Referencia Bibliográfica	Warren, Samuel & Brandeis, Louis. (Diciembre, 1890). The Right to Privacy. Harvard Law Revie. The Harvard Law Review Association, Volumen 4, núm.5, 193-220. Recuperado el 20 de abril de 2015 de: http://www.english.illinois.edu/~people/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf
Tema	Origen histórico del derecho a la intimidad en el ordenamiento jurídico de los Estados Unidos de América
Conceptos Clave	Property, privacy, trademarks, common law, intangible property, trade secrets, defamation, law of slander and of libel.
Idea principal	“It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is.”(P.197)
Ideas secundarias relevantes	<p>“That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. (...) Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses vi et armis ” (P.193)</p> <p>Thus, with the recognition of the legal value of sensations, the protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in fear of such injury. From the action of battery grew that of assault. (...) Similar to the expansion of the right to life was the growth of the legal conception of property. From corporeal property arose the incorporeal rights issuing out of it; and then there opened the wide realm of intangible property, in the products and processes of the mind, as works of literature and art, goodwill, trade secrets, and trademarks. (P.194)</p> <p>The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition,</p>

and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature.(P.195)

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone"(P.195)

The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.(P.196)

It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is.(P.197)

It is not however necessary, in order to sustain the view that the common law recognizes and upholds a principle applicable to cases of invasion of privacy, to invoke the analogy, which is but superficial, to injuries sustained, either by an attack upon reputation or by what the civilians called a violation of honor; for the legal doctrines relating to infractions of what is ordinarily termed the common-law right to intellectual and artistic property are, it is believed, but instances and applications of a general right to privacy, which properly understood afford a remedy for the evils under consideration.(P.198)

The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. (...)The right is lost only when the author himself communicates his production to the public, -- in other words, publishes it. (P.198)

That this protection cannot rest upon the right to literary or artistic property in any exact sense, appears the more clearly when the subject-matter for which protection is invoked is not even in the form of intellectual property, but has the attributes of ordinary tangible property. Suppose a man has a collection of gems or curiosities which he keeps private : it would hardly be contended that any person could publish a catalogue of them, and yet the articles enumerated are certainly not intellectual property in the legal sense, any more than a collection of stoves or of chairs(P.202)

The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.(P.205)

The same protection is afforded to emotions and sensations expressed in a musical composition or other work of art as to a literary composition; and words spoken, a pantomime acted, a sonata performed, is no less entitled to protection than if each had been reduced to writing. The circumstance that a thought or emotion has been recorded in a permanent form renders its identification easier, and hence may be important from the point of view of evidence, but it has no significance as a matter of substantive right. If, then, the decisions indicate a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression.(P.206)

The right of property in its widest sense, including all possession, including all rights and privileges, and hence embracing the right to an inviolate personality, affords alone that broad basis upon which the protection which the individual demands can be rested.(P.211)

Thus, the courts, in searching for some principle upon which the publication of private letters could be enjoined, naturally came upon the ideas of a breach of confidence, and of an implied contract; but it required little consideration to discern that this doctrine could not afford all the protection required, since it would not support the court in granting a remedy against a stranger; and so the theory of property in the contents of letters was adopted(P.211) (...)A similar groping for the principle upon which a wrongful publication can be enjoined is found in the law of trade secrets. There, injunctions have generally been granted on the theory of a breach of contract, or of an abuse of confidence.(P.212)

We must therefore conclude that the rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights as against the world; and, as above stated, the principle which has been applied to protect these rights is in reality not the principle of private property, unless that word be used in an extended and unusual sense. The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise.(P.213)

If the invasion of privacy constitutes a legal injuria, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation.(P.213)

It remains to consider what are the limitations of this right to privacy, and what remedies may be granted for the enforcement of the right. To determine in advance of experience the exact line at which the dignity and convenience of the individual must yield to the demands of the public welfare or of private justice would be a difficult task; but the more general rules are furnished by the legal analogies already developed in the law of slander and libel, and in the law of literary and artistic property.(P.214)

Conclusions

1. The right to privacy does not prohibit any publication of matter which is of public or general interest. In determining the scope of this rule, aid would be afforded by the analogy, in the law of libel and slander, of cases which deal with the qualified privilege of comment and criticism on matters of public and general interest.(...)”(P.214)
The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever; their position or station, from having matters which they may properly prefer to keep private, made public against their will
2. The right to privacy does not prohibit the communication of any matter, though in its nature private, when the publication is made under circumstances which would render it a privileged communication according to the law of slander and libel.(P.216)
3. The law would probably not grant any redress for the invasion of privacy by oral publication in the absence of special damage. The same reasons exist for distinguishing between oral and written publications of private matters, as is afforded in the law of defamation by the restricted liability for slander as compared with the liability for libel (P.217)
4. The right to privacy ceases upon the publication of the facts by the individual, or with his consent.(P.217)
5. The remedies for an invasion of the right of privacy are also suggested by those administered in the law of defamation, and in the law of literary and artistic property, namely:

	<p>1. An action of tort for damages in all cases.[51] Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel.</p> <p>2. An injunction, in perhaps a very limited class of cases.</p>
Análisis conceptual del documento	El artículo analiza la manera como se ha protegido jurídicamente el ámbito privado y familiar de las intromisiones ajenas conforme a varia jurisprudencia tomada de los tribunales norteamericanos.
Aportes del texto	La concepción de la privacidad en el derecho norteamericano, entendido como un derecho a estar solo, a no ser perturbado en la tranquilidad espiritual, que se proyecta en los ámbitos del derecho al buen nombre, al honor, a la honra.
Polémicas	No se encontraron polémicas
Preguntas que suscita el texto	No genera ninguna
Comentario Personal	Ha permitido comprender el modelo de privacidad norteamericano, en sus desarrollos conceptuales originales. Se vincula profundamente a una concepción individualista de protección de las personas que surge a raíz del respeto de la libertad que tienen en su constitución.
Referencia de otros autores	NA

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 10 de 17/03/2016
Propósito del diligenciamiento: Obtener el conocimiento de la evolución histórica de los derechos fundamentales, la fundamentación de los derechos humanos, el desarrollo del derecho a la intimidad en la Constitución española, a manera de derecho comparado, y por último el impacto del derecho a la intimidad dentro de la sociedad de la información, producto de las nuevas herramientas informáticas y tecnológicas	
Referencia Bibliográfica	PÉREZ LUÑO, Antonio Enrique (2005). <i>Capítulo Primero: Delimitación Conceptual de los derechos Humanos</i> . En: Derechos humanos, estado de derecho y Constitución. Madrid: Tecnos.
Tema	Derechos Fundamentales, Derechos Humanos, Intimidad en la Constitución española, Intimidad bajo la informática.
Conceptos Clave	Derechos Humanos, Iusnaturalismo racionalista, derechos fundamentales, libertades públicas, derecho natural, ley natural, ambigüedad lingüística.
Idea principal	Los derechos humanos tienen una gran dificultad: uso de un lenguaje ambiguo que implica muchos significados por los cuales se pasa para formular una que sea general e incluyente.
Ideas secundarias relevantes	<p>“La significación heterogénea de la expresión <<derechos humanos>> en la teoría y en la praxis ha contribuido a hacer de este concepto un paradigma de equivocidad (...) A esa vaguedad de los derechos humanos se ha referido expresamente Norberto Bobbio, para quien en la mayor parte de las ocasiones esta expresión o no es realmente definida, o lo es en términos poco satisfactorios. Teniendo presente su planteamiento se pueden distinguir tres tipos de definiciones:</p> <ol style="list-style-type: none"> Tautológicas, no aportan ningún elemento nuevo que permita caracterizar tales derechos Formales, no especifican el contenido de estos derechos, limitándose a alguna indicación sobre su estatuto deseado o propuesto. Teleológicas, en las que se apela a ciertos valores últimos susceptibles de diversas interpretaciones”

	<p>“La falacia más común en el lenguaje de los derechos humanos consiste en la confusión entre los niveles descriptivo y prescriptivo.(...) Resulta evidente para Bentham la contradicción que existe entre la realidad práctica y esas supuestas facultades de libertad e igualdad que aparecen formuladas en términos descriptivos, como un hecho, cuando no constituyen más que objetivos situados en el plano del <<deber ser>>”(P.29)</p> <p>La ambigüedad del lenguaje afecta más en el plano legislativo, donde “las palabras impropias, que han nacer ideas falsas, pueden conducir a calamidades nacionales”, y resalta la confusión de la palabra <i>derechos humanos</i> con la de libertades públicas, derechos naturales, derechos subjetivos, derechos subjetivos públicos, derechos individuales (30)</p> <p>Los derechos humanos tienen el antecedente histórico del ius naturalismo racionalista. En efecto varios de los doctrinantes quisieron buscar un fundamento más allá del hombre, en principio en Dios y luego en la razón, que resultaba obligatoria para todos los hombres en su actuar para encontrar límites a las arbitrariedades del soberano de turno, garantizando la convivencia humana.</p> <p>“En todo caso, conviene tener en cuenta que los autores de los siglos XVII y XVIII afirmaron[en referencia a esto ver p.41 a 42] la prioridad de los derechos naturales subjetivos sobre el derecho objetivo positivo, pero ninguno de ellos pretendió, lo que hubiera sido un contrasentido, sostener la primacía de los derechos naturales subjetivos sobre el derecho natural objetivo, aunque pusieran el acento sobre los primeros o se ocupasen preferente o exclusivamente de aquéllos”(P.43)</p> <p>“La ley natural, tal como aparece perfilada en la doctrina clásica sobre el particular de Tomás de Aquino, posee, entre otras propiedades, las de su carácter originario, universal e inmutable”(P.43)</p> <p>Antonio Perez Luño define derechos humanos como “un conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, libertad y la igualdad humanas, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional e internacional”(P.50)</p> <p>Es importante resaltar en la anterior definición los conceptos de dignidad, libertad e igualdad para el ser humano. Sobre la dignidad, escribe que consiste en el punto de referencia, el que permite dar el reconocimiento a la personalidad del hombre y sus facultades debido a que lo dimensiona moralmente a la persona. La libertad es la llave que permite las manifestaciones propias del ser humano. Por último la igualdad permite materializar el acceso a las oportunidades por parte de todos, variando los niveles de libertad formal hacia una libertad material.</p>
Análisis conceptual del documento	El capítulo se centra en realizar una exposición sobre el origen diverso del concepto de derechos humanos, lo que implica un uso confuso de esta palabra, variedad de definiciones y una mezcla con otras nociones jurídicas como derechos fundamentales, derecho natural, libertades públicas para concluir en una definición base de derechos humanos
Aportes del texto	La definición que concluye de derechos humanos como “conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, libertad y la igualdad humanas, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional e internacional”(P.50)
Polémicas	Los diversos significados de la palabra derechos humanos y los motivos por los cuales son reconocidos como tales son una fuente de desacuerdo entre los estudiosos.
Preguntas que suscita el texto	NA
Comentario Personal	El marco conceptual inicial para que puedan distinguirse los derechos humanos de otros conceptos jurídicos y filosóficos con los que tiende a mezclarse es el aporte concluyente del profesor Pérez Luño.

Referencia de otros autores	Locke, J. <i>Two treatises of government.</i> (Trad. Al español como <i>Dos tratados sobre del gobierno</i>)
-----------------------------	--

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR :	Camilo José Puello Rincón
	GUIA N° 11 de 19/03/2016
Propósito del diligenciamiento: Falta realizar el análisis de este capítulo según esta ficha, ver P.54 del libro para iniciar.	
Referencia Bibliográfica	PÉREZ LUÑO, Antonio Enrique (2005). <i>Capítulo Segundo: El proceso de positivación de los derechos fundamentales.</i> En: Derechos humanos, estado de derecho y Constitución. Madrid: Tecnos.
Tema	Realismo jurídico, positivismo jurídico, iusnaturalismo,
Conceptos Clave	Origen de los derechos humanos, corrientes de estudio, derechos naturales, derechos públicos subjetivos
Idea principal	Se busca describir el proceso jurídico de positivación de los derechos humanos y su incidencia en el proceso de formación de las reglas jurídicas.
Ideas secundarias relevantes	<p>“Si la lucha por el reconocimiento de la dignidad de la persona humana puede considerarse como una constante en la evolución de la filosofía jurídica y la política humanista, la tendencia a la positivación de las facultades que tal dignidad entraña se puede considerar como una inquietud estrechamente ligada a los planteamientos doctrinales de la hora presente”(P.55)</p> <p><i>Tesis iusnaturalistas</i></p> <p>Bajo el rótulo de iusnaturalismo se han agrupado históricamente una serie de doctrinas heterogéneas e incluso contradictorias, que han servido para defender y fundamentar la existencia del derecho natural (...) Ahora bien, las distintas concepciones iusnaturalistas si en algo han coincidido ha sido en afirmar la existencia de unos postulados de juridicidad anteriores y justificadores del derecho positivo. (...) Las teorías iusnaturalistas coinciden en contemplar el proceso de positivación de los derechos humanos como la consagración normativa de unas exigencias previas, de unas facultades que le corresponden al hombre por el mero hecho de serlo (...) Desde esta perspectiva la positivación asume un carácter puramente declarativo, y será considerada como la culminación de un proceso que tiene su origen en las exigencias que la razón postula como imprescindibles para la convivencia social. (...) En las principales Declaraciones del siglo XVIII, fruto de la inspiración iusnaturalista, se advierte también el sentido declarativo que en ellas asumía la positivación de los derechos fundamentales.”(P.56-57)</p> <p><i>Tesis positivistas</i></p> <p>“Cualquier creencia en normas objetivamente válidas anteriores a tal derecho aparece como el producto de una posición metafísica e inaceptable. De ahí que el proceso de positivación sea entendido por los positivistas como un aspecto más de las reglas generales que presiden la creación del derecho en el ordenamiento estatal”(P.58)</p> <p>“Las razones por las que se desea que existan esos derechos no constituyen de por sí derechos, del mismo modo que el hambre no crea el pan”(Bentham, cit. en P.58)</p> <p>“El progresivo descrédito de la teoría de los derechos naturales en la ciencia jurídica alemana de finales del siglo XIX y principios de nuestro siglo, motivado en gran parte por la crítica del positivismo jurídico, determinó la aparición de una nueva categoría: los derechos públicos subjetivos. (...)En efecto, la nueva categoría se presentará como intento</p>

de ofrecer una configuración jurídico-positiva, de la exigencia mantenida por la teoría de los derechos naturales de afirmar las libertades del individuo frente a la autoridad del Estado. Para eso se precisaba de unas estructuras del poder de forma que fuera posible la instauración de relaciones jurídicas entre el Estado y los particulares, para lo que se debía reconocer la personalidad jurídica del Estado, que de este modo adquiriría la titularidad de derechos y obligaciones para con los ciudadanos, estableciéndose también una consiguiente tutela jurisdiccional de las situaciones subjetivas así instituidas”(P.59)

“En opinión de Jellinek la pertenencia al Estado califica a cada ciudadano y se concreta en una serie de relaciones que lo colocan en diversas situaciones jurídicas (*Zustände*), de las que surgen pretensiones jurídicas (*Ansprüche*). Estas pretensiones de los ciudadanos constituyen los derechos públicos subjetivos, los cuales han ido afirmándose progresivamente en cuatro fases o statuts.” (P.60)

“El problema de la positivación será visto siempre desde estas premisas no como un acto de reconocimiento o declarativo, sino como un acto de creación y, por tanto constitutivo. Con anterioridad a la positivación podrán reconocerse expectativas de derecho o postulados sociales de justicia, pero nunca derechos”(P.60)

Tesis realistas

“Integran este grupo quienes no otorgan al proceso de positivación un significado declarativo de derechos anteriores (tesis iusnaturalista), o constitutivo (tesis positivista), sino que entienden que tal proceso supone un requisito más a tener en cuenta para el efectivo y real disfrute de tales derechos. La positivación no se considera, por tanto el final de un proceso, sino una condición para el desarrollo de las técnicas de protección de los derechos fundamentales, que son las que en definitiva definen su contenido(...) Por ello la actitud realista implica una crítica de iusnaturalismo(en especial de sus versiones racionalistas del siglo XVIII) por su concepción ideal de los derechos humanos y del positivismo jurídico por su consideración puramente formal de los mismos”(P.61)

“La positivación es considerada desde este enfoque como un instrumento que permite definir mejor y concretar el alcance de esos derechos; pero, en todo caso, son las condiciones sociales las que determinan el sentido real de los derechos y libertades, pues de ellas depende su salvaguardia y protección”(P.63)

“En esta dirección pueden situarse, por ejemplo las tesis que conciben la protección procesal de los derechos fundamentales como el factor clave de su significación”(P.63)

“Como resumen de lo expuesto puede advertirse que, mientras el iusnaturalismo sitúa el problema de la positivación de los derechos humanos en el plano filosófico y el positivismo en el jurídico, para el realismo se inserta en el terreno político, aunque también, como se ha visto, otorgue una importancia decisiva a las garantías jurídico-procesales de tales derechos”(P.64)

3. Marco institucional de la positivación

“Hasta aquí se ha venido estudiando el problema de la positivación de los derechos fundamentales a través de su enfoque desde diversos planteamientos doctrinales, pero como adelantaba, junto a este nivel de consideración resulta imprescindible tener presente su plasmación en diversas instituciones y normas jurídico-positivas (...) tiende a ponder de relieve la existencia del principio de organización que rige a un conjunto de elementos que se condicionan recíprocamente, la dimensión genética o diacrónica de un proceso tan sólo puede ser comprendida tras su previa formalización a partir del análisis

sincrónico”(P.64)

“El análisis sincrónico de la positivación de tales derechos tiene por objeto el estudio de las técnicas a través de las cuales se ha realizado en el seno de los distintos ordenamientos jurídicos”(P.65)

“A partir del siglo XVIII se considera un postulado fundamental del régimen liberal reservar al poder constituyente, en cuanto titular de la soberanía popular, el privilegio de fijar los derechos básicos de convivencia social, bien mediante su inserción en el preámbulo de las constituciones, o en su texto articulado o, incluso, en una declaración específica de tales derechos. No en vano, para el pensamiento liberal el fin supremo de cada asociación política residía en la defensa de las libertades fundamentales, para cuya mejor garantía estas debían proclamarse expresamente en las normas de mayor rango y autoridad del ordenamiento jurídico”(P.67)

“Debe advertirse que a los efectos de esta investigación las declaraciones de derechos y los preámbulos poseen una significación similar. Se trata en ambos casos de enunciar, por parte del constituyente, los grandes principios rectores de la vida política.”(P.73)

“Como resumen de lo expuesto parece que puede desprenderse la tesis de que todas las disposiciones sobre derechos fundamen tales contenidas en un texto constitucional, sea en su articulado, o en su preámbulo, o en una declaración independiente de igual rango, son manifestaciones positivas de juridicidad. El criterio material determinará, en cada caso, si la positivación , reviste el carácter de un precepto o el de un principio general y fundamental del derecho”(P.79)

“Principios originariamente dirigidos a poner límite a la actuación del Estado se han convertido en normas que exigen su gestión en el orden económico y social; garantías pensadas para la defensa de la individualidad son ahora reglas en las que el interés colectivo ocupa el primer lugar; enunciados muy precisos sobre facultades que se consideraban esenciales y perennes han dejado paso a normas que defienden bienes múltiples y circunstanciales”(P.85)

“Un importante sector de la doctrina alemana ha llegado incluso a afirmar que en la compleja sociedad actual los derechos del individuo tan sólo pueden tener justificación como derechos sociales. Sin que ello signifique una negación de los valores de la personalidad, sino una superación de la imagen de unos derechos del individuo solitario que decide de forma insolidaria su destino, para afirmar la dimensión social de la persona humana, dotada de valores autónomos pero ligada inescindiblemente por numerosos vínculos y apremios a la comunidad en la que desarrolla su existencia”(P.90)

“El realismo más elemental obliga a reconocer que las libertades puras, aquellas cuyo disfrute sólo dependería de la abstención del Estado, se hallan irremediamente superadas por la evolución económica y social de nuestro tiempo. ¿Qué sería – se pregunta Burdeau – de la libertad de circulación sin un código del tráfico, de la libertad de cultos sin las subvenciones, para el mantenimiento de los templos, de la libertad de prensa sin privilegios fiscales para los periódicos...? (P.93)

“Un problema más arduo es el que se refiere a la titularidad de los derechos sociales y su eficacia frente a terceros. Ya que, en muchas ocasiones, el Estado no realiza directamente las obligaciones que se derivan de estos derechos (...) El problema ha sido abordado con especial atención por la doctrina y la jurisprudencia alemana en relación con la denominada Driuwirkung der Grundrechte (eficacia frente a terceros de los derechos fundamentales). Se trata, en suma, de la aplicación de los derechos fundamentales no sólo en las relaciones entre el Estado y los ciudadanos, sino también en las relaciones entre personas privadas” (P. 94-95)

	“En los esquemas del pensamiento liberal al juez no le correspondían funciones creadoras y mucho menos en el terreno de las libertades fundamentales en el que el juez debía limitarse a aplicar estrictamente aquellas normas generales y previamente sancionadas en las que éstos venían promulgados.(...) Gran parte de la doctrina y la jurisprudencia germana entiende que el principio tradicional de la división de poderes, según se recoge en la <i>Grundgesetz</i> , no debe interpretarse como exigencia de una rígida separación, sino como la de un control y colaboración recíproco entre todos los poderes que ejercen funciones estatales para lograr una coordinación armónica en sus tareas. Por ello, tal principio debe ser completado por el de subsidiariedad, en virtud del cual, cuando los órganos legislativos no asumen la tarea de desarrollar y completar positivamente las disposiciones constitucionales, tal tarea puede ser realizada por el juez”(P.106-106)
Análisis conceptual del documento	Para comprender el proceso de positivación de los derechos humanos debe entenderse los momentos históricos por los cuales ha pasado cada uno, el tipo de norma que los ha regulado y la forma de la redacción. Con estos tres elementos se puede comprender que todo el proceso ha sido ascendente, desde unas normas sin mayor vinculación jurídica y gran ambigüedad en sus términos, hasta las actuales donde se consagran en textos llamados Constituciones y se les establece su vinculatoriedad por todos los poderes públicos y privados, garantizando esto último a través de medios procesales.
Aportes del texto	El texto permite comprender los distintos niveles de positivación y las teorías jurídicas que explican el fenómeno al respecto.
Polémicas	NA
Preguntas que suscita el texto	NA
Comentario Personal	Este documento permitió ampliar la visión sobre el papel del Estado en la garantía actual de los derechos fundamentales, representa un aporte en algunas de sus ideas a mi trabajo de grado.
Referencia de otros autores	NA

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 12 de 05/04/2016
Propósito del diligenciamiento: Obtener una comprensión amplia del proceso jurídico que atravesó el Estado en sus múltiples fases: desde el inicio en el Estado de Derecho, luego el Estado Social de Derecho y finalmente el llamado Estado Social y Democrático de Derecho	
Referencia Bibliográfica	PÉREZ LUÑO, Antonio Enrique (2005). <i>Capítulo 5: Estado social y democrático de derecho y derechos fundamentales</i> . En: <i>Derechos humanos, estado de derecho y Constitución</i> . Madrid: Tecnos.
Tema	El desarrollo histórico del Estado de derecho hasta el último estadio y una corta definición al respecto
Conceptos Clave	Estado social de derecho, derechos fundamentales, estado de derecho, derechos humanos, análisis histórico.
Idea principal	La clave es entender la relación entre el componente ideológico que busca una justicia social, ante las inequidades, para garantizar la convivencia social y el componente técnico jurídico que pretende crear un clima de seguridad jurídica para el desarrollo de la actividad humana a través de la expedición válida de normas.
Ideas secundarias relevantes	“En su perspectiva histórica la teoría de los derechos fundamentales precede a la formulación doctrinal de la noción del Estado de derecho (P.218) (...) no es menos cierto que éstas no pueden alcanzar su formulación positiva al margen del ordenamiento jurídico del Estado. Si bien los derechos fundamentales, encarnan, a su vez, los principios inspiradores de toda la política estatal. Por lo que cumplen una misión de fundamento y límite de todas las normas que organizan el funcionamiento de los poderes públicos, y, en suma, de todas las experiencias concretas de juridicidad surgidas en el seno del ordenamiento en que se

	<p>formulan.”(P.219)</p> <p>“Existe un amplio acuerdo (...) en cifrar el origen moderno de esta idea en la filosofía política de Inmanuel Kant. No existe en cambio unanimidad a la hora de explicar y valorar el significado de esta aportación kantiana.”(P.220)</p> <p>“a) Kant acepta, en principio, la tesis del iusnaturalismo iluminista de que el Estado es un medio y una condición para asegurar las respectivas esferas de libertad de los ciudadanos por medio del derecho (...) su objetivo prioritario la garantía de la libertad a través del derecho. “La concepción que se desprende de esta tesis es la del derecho como condición de coexistencia de las libertades individuales, que atribuye al Estado la garantía, mediante su no injerencia, del libre desarrollo de la libertad”(P.221)</p> <p>“b)(...) Kant emplea el término de libertad en sentido positivo, como autonomía o participación de los ciudadanos en la elaboración de las normas que deben regular su conducta”(P.222) Ayudado por la idea de contrato social, que permite aglutinar a todas las personas con el ideal de un solo legislador que hubiese expresado la voluntad conjunta del pueblo. “Lo que el hombre pierde con el contrato social es su libertad natural y un derecho ilimitado a cuanto le apetezca y pueda alcanzar; lo que gana es la libertad civil y la propiedad de todo lo que posee”(P.222)</p> <p>Kant considera que existe una serie de tres leyes que permiten la constitución del Estado según la pura razón: 1) La libertad de cada miembro de la sociedad, como hombre; 2) La igualdad de él mismo frente a cualquier otro, como súbdito; 3) La independencia de cada miembro de la comunidad, como ciudadano” (P.222)</p> <p>“La diversidad de planos en los que opera la reflexión kantiana sobre el Estado reflejan puntualmente las distintas acepciones de la libertad que, como he indicado, han dejado lugar a un interesante debate hermenéutico en torno a su filosofía jurídico-política”(P.223)</p> <p>“El reproche que pueda hacerse a su legitimación del poder, en la práctica, omnipotente del soberano, de su culto a la legalidad, de su negación del derecho de resistencia, encuentra su respuesta en la observación de que tales presupuestos constituyen una consecuencia lógica del carácter racionalmente necesario del Estado para la realización del derecho”(P.224)</p> <p>“A partir de Humboldt la teoría del Estado de derecho irá perdiendo, sin embargo su pretendido carácter formal-racional para ir llenándose de un contenido político y expresamente manifestado: la ideología liberal”(P.225)</p> <p>“El estado de Derecho nació, por tanto, como una fórmula de compromiso que implicaba aunar diversas <i>garantías formales</i>, proclamadas por una Constitución que consagra la división de poderes y el principio de legalidad, con una serie de <i>garantías materiales</i>, ya que el primado de la ley reposaba en su carácter de expresión de la voluntad general y en su inmediata orientación a la defensa de los derechos y libertades de los ciudadanos. Incluso se ha llegado a afirmar que, en estas formulaciones iniciales del Estado de Derecho, la noción de legalidad suponía una síntesis de la <i>idea liberal</i> manifestada en la defensa de los derechos individuales, con la <i>idea democrática</i> concretada en la concepción de la ley como producto de la voluntad general”(P.226)</p> <p>“Hegel opone la idea democrática de soberanía popular, que, a su entender, reposa en una imagen confusa y vacua del pueblo, una soberanía estatal que concibe al pueblo como totalidad orgánica y se realiza en la persona del monarca. El estado ético termina así por convertirse en lo que certeramente calificó Hermann Heller como Estado de fuerza.”(P.228)</p> <p>“Una importancia mucho mayor, para la conformación de la idea del Estado de Derecho, debe reconocerse en la progresiva influencia del positivismo jurídico formalista en la teoría germana del derecho público(...) pasará a convertirse en un estado limitado por el derecho positivo, es decir, un estado que se autolimita”(P.228)</p>
--	---

	<p>“La teoría del Estado de Derecho forjada (...) constituye la expresión más acabada del Estado Liberal de Derecho. Sus rasgos definitorios pueden cifrarse en:</p> <ul style="list-style-type: none"> a) Una aparente despolitización del Estado, que, lejos de proponerse la realización de fines políticos propios, aparece como un mero instrumento neutro y disponible (...) para garantizar jurídicamente el libre juego de los intereses económicos” b) Tendencia hacia la identificación del concepto de Estado de Derecho con el principio de legalidad, lo que implica el sometimiento de la administración a la ley, así como la posibilidad del control jurisdiccional de sus actos”(P.228-229) <p>“El individualismo, así como el apoliticismo y neutralidad del Estado liberal de Derecho, no podía satisfacer la exigencia de libertad e igualdad reales de los sectores social y económicamente más deprimidos”(P.229) “(...) es decir, responsabiliza a la Administración de la tarea de proporcional a la generalidad de los ciudadanos las prestaciones necesarias (...) para el pleno desarrollo de su personalidad reconocida no sólo a través de las libertades tradicionales, sino también a partir de la consagración constitucional de los derechos fundamentales de carácter económico, social y cultural”(P.231)</p> <p>Existieron críticas contra este Estado volcado a lo social que se resumen así: “(...) en su evolución histórica el elemento definitorio del Estado de Derecho aparece ligado a la Constitución, mientras que la función social del Estado es algo que se vincula a las tareas propias de la Administración”(P.221)</p> <p>“ El abandono de la concepción formalista del Estado de Derecho, de signo marcadamente conservador, no implica, por tanto, sustraer la actividad de los poderes públicos del sometimiento estricto al principio de legalidad, sino que tiene a evitar que la normatividad constitucional pueda quedar vacía de contenido o falta de eficacia”(P.235)</p> <p>Estos adjetivos al Estado de derecho han influido en el uso lingüístico de la expresión. “En su acepción <i>técnica</i> (...) pretende dar cuenta de unos mecanismos o condiciones jurídicos (...) que presiden el funcionamiento del estado (...) Los presupuestos fundamentales sobre los que gravita esta concepción son: limitación de la actividad de los órganos del poder sobre la legalidad; la garantía por parte de ésta de los derechos públicos subjetivos, que adquieren tal cualidad por su positivación (...); y la teoría de la forma o control jurisdiccional del Estado.”(P.245) “Desde este plano ideológico la fórmula “Estado de derecho” ha sido un caballo de batalla para la lucha, en ocasiones ideal y utópica, por el perfeccionamiento de la realidad empírica del Estado”(P.246)</p> <p>“Para dotar a la noción de “Estado de Derecho” de un status significativo preciso y, consiguientemente, para comprender su relevancia en la teoría y en la praxis política, es necesario reconocer en ella una tensión entre las garantías formales que la integran y las exigencias material de la justicia que la presentan como elemento de legitimación” (P247). “En todo caso las exigencias de justicia material implícitas en el desarrollo histórico del iusnaturalismo siguen siendo una vieja aspiración insatisfecha de la humanidad. Esa aspiración constituye, a mi entender, el motor de la lucha por el Estado de Derecho, y a ella deben referirse los medios técnicos con que dicha fórmula política se dirige a conseguir sus objetivos, que explícita o implícitamente rebasan siempre el ámbito de las meras garantías formales”(P.249)</p> <p>La clave es entender la relación entre el componente ideológico que busca una justicia social, ante las inequidades, para garantizar la convivencia social y el componente técnico jurídico que pretende crear un clima de seguridad jurídica para el desarrollo de la actividad humana a través de la expedición válida de normas.</p>
Análisis conceptual del	El presente documento expresó unas ideas interesantes acerca de la evolución del Estado de Derecho, los aspectos históricos que influyeron en su configuración inicial, su componente

documento	social y luego constitucional. Finalmente como hay una implícita necesidad entre Estado de derecho y derechos fundamentales en la época actual.
Aportes del texto	El aporte de este texto consistió en algunas ideas acerca de la relación que existe entre Estado de Derecho y derechos fundamentales.
Polémicas	NA
Preguntas que suscita el texto	NA
Comentario Personal	NA
Referencia de otros autores	NA

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N°13 de 11/04/2016
Propósito del diligenciamiento: Comprender como encaja el derecho a la protección de datos personales en la tercera generación de los derechos humanos y los motivos por los cuales históricamente se sitúa de esta manera.	
Referencia Bibliográfica	Pérez Luño, A. (2006) La tercera generación de derechos humanos. Navarra: Aranzadi. CapítuloS 1,2,3,4 y 9
Tema	Los derechos humanos surgidos a raíz de los hechos ocurridos en el siglo XX.
Conceptos Clave	Generaciones de derechos humanos, derechos individuales, universalismo de los derechos humanos, derechos subjetivos,
Idea principal	Los derechos humanos han nacido con unos perfiles ideológicos definidos, “que tan sólo pueden predicarse con sentido en contextos temporalmente determinados (...)”
Ideas secundarias relevantes	<p>“Los derechos y libertades de la tercera generación se presentan como una respuesta al fenómeno de la denominada “contaminación de las libertades (liberties’ pollution) término con el que algunos sectores de la teoría social anglosajona aluden a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías”(P.29)</p> <p>“En efecto, cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida, que afecta potencialmente incluso a los aspectos más sensibles de su vida privada; aquellos que en épocas anteriores quedaban fuera de todo control por su variedad y multiplicidad”(P.31)</p> <p>“En una sociedad como la que nos toca vivir en la que la información es poder y en la que ese poder se hace decisivo cuando, en virtud de la informática, convierte informaciones parciales y dispersas en masa y organizadas, la reglamentación jurídica de la información reviste un interés prioritario”(P.32)</p> <p>Capítulo II. Estado constitucional y derechos de la tercera generación</p> <p>“En algun caso la referencia en favor de la fórmula “estado constitucional” respecto a la de “estado de derecho”, se justifica como un marco de referencia más adecuado para un tratamiento de la problemática estatal situado “en el ámbito jurídico”; aunque expresamente se indicará que esa opción se realiza “sin perjuicio de reconocer la fluidez de uno y otro concepto” (Pérez Luño,2006:51)</p> <p>“A tenor de ello entiendo que la decantación terminológica desde el estado de derecho al estado constitucional puede considerarse el reflejo de un triple desplazamiento advertible en</p>

	<p>los ordenamientos jurídicos de los sistemas democráticos que se concreta en:</p> <ol style="list-style-type: none"> 1) El desplazamiento desde la primacía de la ley a la primacía de la constitución 2) El desplazamiento desde la reserva de ley a la reserva de constitución 3) El desplazamiento desde el control jurisdiccional de la legalidad al control jurisdiccional de la constitucionalidad”(Pérez Luño,2006:53) <p>“El pluralismo jurídico implica una derogación de las ideas de monopolio y jerarquía normativa, así como una erosión inmediata del protagonismo de la ley”(Pérez Luño, 2006:54) “(…) en función de lo que se denominan “sistemas de interlegalidad”, o sea, de la intersección de sistemas de áreas y niveles jurídicos sobrepuestos e interrelacionados de forma asimétrica y asistemática, a partir de múltiples redes de juridicidad” (Pérez Luño, 2006:55)“Para reconducir esos fenómenos e intentar poner en orden el caos normativo que amenaza con abolir por entero la unidad, coherencia y jerarquía del sistema de fuentes del derecho, hoy se vuelven los ojos hacia la Constitución (…) norma máxima del ordenamiento jurídico, garantiza la conformidad a su contenido de todas las normas restantes y la consiguiente nulidad de las que la contradicen” (Pérez Luño, 2006:56)</p> <p>El parlamento anteriormente tenía la competencia exclusiva para regular el ordenamiento jurídico en sus aspectos más esenciales e importantes, esto cambió cuando se procuró la satisfacción existencial de las personas a través de la presencia creciente del Estado con sus órganos administrativos y la intervención legal. Ahora es la Constitución quien asigna las competencias para que desarrollen las cuestiones constitucionales básicas a través de la reserva de la constitución.(Pérez Luño, 2006:59)</p> <p>La tutela de la intimidad dada inversamente a su dimensión social como actividad compartida es artificiosa, debe cambiarse a un sistema basada en la intensidad social de la conducta confrontada con el deseo de la persona de mantener sus datos en el plano de reserva. (Pérez Luño, 2006:134)</p>
Análisis conceptual del documento	Los derechos humanos de la tercera generación han sido formulados como reacción, frente a la fuerte influencia las nuevas tecnologías el ejercicio de las libertades individuales y tienen relación con los fenómenos de la constitucionalización del derecho y el pluralismo jurídico.
Aportes del texto	<p>La formulación histórica de los derechos humanos sin que ello le reste la universalidad, que el autor formula como un deber ser en constante búsqueda para alcanzarla.</p> <p>La teoría del <i>status</i> de Jellinek se propone como adecuada para describir las situaciones subjetivas que padecen los derechos humanos, aunque ampliándola para incluir a la tercera generación como un status diferente.</p> <p>“(…) [L]a relevancia que ahora asumen las normas de procedimiento para la organización y realización de los derechos humanos hace que se aluda a un <i>status activus processualis</i>. Erhard DENNINGER concibe dicho <i>status</i> como el reconocimiento de la facultad de cada persona para participar activamente y asumir su propia responsabilidad en los procedimientos que le afectan, así como en el seno de las estructuras organizativas más directamente vinculadas con el ejercicio de los derechos fundamentales” (Pérez Luño, 2006:37)</p> <p>“En algún caso la referencia en favor de la fórmula “estado constitucional” respecto a la de “estado de derecho”, se justifica como un marco de referencia más adecuado para un tratamiento de la problemática estatal situado “en el ámbito jurídico”; aunque expresamente se indicará que esa opción se realiza “sin perjuicio de reconocer la fluidez de uno y otro concepto” (Pérez Luño,2006:51)</p> <p>“Para HÄBERRLE el estado constitucional es un arquetipo jurídico-político en el que los poderes públicos se hallan conformados y limitados por el derecho a través de principios constitucionales formales y materiales: los derechos fundamentales, la función social de las instituciones, la división de los poderes y la independencia de los tribunales.” (Pérez Luño,</p>

	<p>2006:67)</p> <p>“El enfoque que propongo tiende a establecer un paralelismo simétrico entre evolución de las formas de Estado de derecho y la decantación de uno de sus ingredientes definitorios básicos: los derechos fundamentales. (...) A las tres generaciones de Estados de derecho corresponden por tanto, tres generaciones de derechos fundamentales. (...) El estado constitucional, en cuanto a Estado de derecho de la tercera generación, delimitará el medio espacial y temporal de paulatino reconocimiento de los derechos de la tercera generación” (Pérez Luño, 2006:74-75)</p> <p>“En su polaridad positiva, Internet supone un vehículo potenciador de las libertades de expresión y comunicación de datos e ideas, que se consideran derechos irrenunciables de las sociedades políticas democráticas contemporáneas y, en concreto, de la UE. Pero, en su polo negativo, se vislumbran riesgos inquietantes en relación con usos abusivos de Internet que directamente menoscaban el ámbito íntimo de los ciudadanos” (P.113)</p>
Polémicas	NA
Preguntas que suscita el texto	¿El derecho a la autodeterminación informática encaja en la solidaridad como su valor guía?
Comentario Personal	NA
Referencia de otros autores	<p>Dworkin, R.(1977). Los Derechos en serio. Barcelona: Ariel.</p> <p>García Pelayo, M. Estado legal y estado constitucional de derecho, en <i>Obras Completas Vol. 3</i>, Madrid: CEC.</p> <p>Haberle,P.(.) Estado constitucional</p> <p>Tribunal Constitucional Alemán. Sentencia del 12 o 15? de diciembre de 1983.</p> <p>Tribunal Constitucional Español. Sentencia 254 del 20 de julio de 1993</p> <p>Tribunal Constitucional Español. Sentencia 231/1988.</p> <p>Tribunal Constitucional Español. Sentencia 290 y 292 de 30 de noviembre de 2000.</p> <p>Tribunal Constitucional Español. Setencia 202/1999.</p> <p>Union Europea.Tribunal de Justicia, sentencia del 6 de noviembre de 2003, asunto C-101/01.</p> <p>Union Europea. Carta de los derechos fundamentales de la Unión Europea. Artículos 7 y 11.</p>

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N°14 de1 15/05/2016
Propósito del diligenciamiento: Comprende el desarrollo del derecho a la intimidad a través del interés de la tutela jurídica a lo largo del siglo XX y su desarrollo en el derecho constitucional español	
Referencia Bibliográfica	PÉREZ LUÑO, Antonio Enrique (2005). <i>Capítulo 8: La intimidad como derecho fundamental</i> . En: Derechos humanos, estado de derecho y Constitución. Madrid: Tecnos.
Tema	Derecho a la intimidad,derecho fundamental.
Conceptos Clave	Generaciones de derechos humanos, derechos individuales, universalismo de los derechos humanos, derechos subjetivos,
Idea principal	“Es notorio que las legislaciones más sensibles a la defensa de las libertades han intentado ofrecer una respuesta jurídica eficaz a una de las exigencias más acuciantes que hoy gravita sobre la sociedad tecnológicamente avanzada: el respeto a la intimidad”(P.323)
Ideas secundarias relevantes	<p>“No debe, por tanto causar problemas que gran parte de las incertidumbres y confusiones que acompañan al tratamiento teórico del derecho al honor, a la intimidad y a la propia imagen nazcan de presuponer, como evidentes por sí, nociones que, como la de dignidad humana le sirven de punto de referencia y fundamento” (P.324)</p> <p>“La dignidad humana constituye no sólo la garantía negativa de que la persona no va a ser objeto de ofensas o humillaciones, sino que entraña también la afirmación positiva del pleno</p>

	<p>desarrollo de la personalidad de cada individuo. El pleno desarrollo de la personalidad supone, a su vez, de un lado, el reconocimiento de la total <i>autodisponibilidad</i>, sin interferencias o impedimentos externos, de las posibilidades de actuación propias de cada hombre; de otro, la <i>autodeterminación (selbstbestimmung des Menschen)</i> que surge de la libre proyección histórica de la razón humana, antes que de una predeterminación dada por la naturaleza”(P.324)</p> <p>“Un aspecto importante de la noción de dignidad humana propuesta por Maihofer es el de partir para la elaboración de su significado de la situación básica (<i>Grundsituation</i>) del hombre en su relación con los demás, esto es, de la situación del ser con los otros (<i>Mitsein</i>); en lugar de hacerlo en función del hombre singular encerrado en su esfera individual (<i>Selbstsein</i>), que había servido de punto de partida para numerosas caracterizaciones de esta idea. Esta dimensión intersubjetiva de la dignidad es de suma trascendencia para calibrar el sentido y alcance de los derechos fundamentales que encuentran en ella su principio fundamentador. La dignidad humana, de otro lado, se identifica con lo que también en ocasiones se denomina libertad moral y se halla estrechamente relacionada con la igualdad, entendida como paridad de estimación social de las Personas. Con lo que se prueba la íntima conexión de los valores que configuran el núcleo conceptual de los derechos humanos”(P.324, Resumen)</p> <p>“De ahí que represente [la dignidad] el principio legitimador de los denominados “derechos de la personalidad”. (...) En efecto, cuando tras el triunfo de la Revolución burguesa se inicia el proceso de positivación de los derechos naturales, bajo la fórmula moderna de los derechos subjetivos, se pretende elaborar un instrumento técnico para la protección de los intereses patrimoniales y, en especial, de la propiedad. Por ello, el derecho subjetivo en sus primeras manifestaciones dogmáticas aparece como un poder de dominio sobre las cosas” (P.325)</p> <p>“Este planteamiento implicaba, en la práctica, la indefensión de los atributos o manifestaciones más íntimamente vinculados a la subjetividad, Para intentar resolver esta situación Otto von Gierke construyó las premisas doctrinales, a finales del pasado siglo de un derecho general de la personalidad, concibiéndolo como el marco unitario de referencia de cuanto pudiera afectar a la libre actuación de la personalidad en todas las direcciones” (P.325)</p> <p>“La construcción de un derecho unitario de la personalidad ha encontrado importantes reservas doctrinales y tesis abiertamente críticas, que han insistido en la necesidad de no extender la protección de la personalidad más allá de los límites de la pluralidad de unos objetos o bienes precisos e individualizables. En efecto, como se ha indicado, la formulación moderna del derecho subjetivo surge como un intento de ofrecer un cauce técnico para el pleno ejercicio del dominio y disfrute de las cosas objeto del derecho de propiedad. Por ello, en sus primeras manifestaciones quedan fuera de su órbita los derechos de la personalidad”(P.326) “Por eso, estos derechos se van incorporando progresivamente al sistema de relaciones jurídicas intersubjetivas, pero, ahí se da una nueva paradoja fruto de la ideología latente en la dogmática (...) se considera que la mejor forma de defender los derechos de la personalidad es la de considerarlos como objetos de propiedad privada, extendiendo a ellos los instrumentos pensados para la tutela externa del derecho de propiedad” (P.327)</p> <p>“En suma, la prevalencia del punto de vista “propietario” ha condicionado el planteamiento de la tutela de la personalidad, en la misma medida en que la idea de la proyección hacia el mundo externo de la personalidad ha funcionado como principio legitimador de la propiedad. “(P.327, Conclusión de sección)</p>
Análisis conceptual del documento	NA
Aportes del texto	NA

Polémicas	NA
Preguntas que suscita el texto	NA
Comentario Personal	NA
Referencia de otros autores	NA

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N°15 de 16/05/2016
Propósito del diligenciamiento: Analizar la forma como el profesor Nelson Remolina describe los tipos de dato personal que reconoce el ordenamiento jurídico colombiano.	
Referencia Bibliográfica	Remolina Angarita, Nelson (2013). <i>Capítulo V, Del dato personal y su clasificación</i> . En: Tratamiento de datos personales, aproximación internacional y comentarios a la Ley 1581 de 2012. Bogotá: Legis S.A.
Tema	Las clases de dato personal que existen en el ordenamiento jurídico colombiano
Conceptos Clave	Persona natural, dato personal, tipos de dato personal, Ley 1581
Idea principal	“La definición de dato personal es necesaria para determinar la aplicación de la LEDP y su clasificación es imprescindible para establecer los requisitos que se deben observar para tratar adecuadamente la información”(P.133)
Ideas secundarias relevantes	<p>“Toda clasificación que se intente hacer respecto de la calidad de los datos depende de la sensibilidad de estos”(P.136)</p> <p>“Las pautas, procesos o protocolos que debe observar el tratamiento de determinada información personal dependen de la naturaleza del dato(...) para que (...) el responsable o encargado adopte las medidas concretas que deben impregnar el tratamiento de determinados datos personales”(P.136)</p> <p>La información personal puede ser clasificada bajo múltiples criterios. Se sigue el que adoptó la ley que tiene en cuenta la accesibilidad y la sensibilidad de la información.</p> <p>Los datos sensibles son aquellos relativos a la salud, a la vida sexual y a los datos biométricos. Pero estos no son taxativos y el criterio de interpretación es que sean datos susceptibles de afectar derechos o libertades fundamentales. Sólo pueden tratarse bajo 5 supuestos enunciados en el artículo 6 de la ley 1581 de 2012.</p> <p>Los datos biométricos representan una posibilidad de avanzar en las investigaciones científicas, también una manera de garantizar la seguridad en muchos espacios públicos, pues rápidamente permitiría identificar criminales que están huyendo de la justicia. “Con los mecanismos biométricos de identificación se captura, procesa y almacena información relacionada con los rasgos físicos de las personas (...) para poder establecer o “autenticar” la identidad de cada sujeto”(P.163)</p> <p>“Algunos datos inicialmente son catalogados como privados, en ciertas ocasiones y en determinados escenarios adquieren la naturaleza de públicos. En este sentido, existe una especie de “relativismo” de la información privada, en la medida que <u>dependiendo de dónde se recolecte</u>, requerirá o no autorización del dato” (P.168)</p>
Análisis conceptual del documento	Los datos personales requieren de una clasificación especial dadas las consecuencias variadas que tiene un tratamiento indebido para cada uno de ellos, adicionalmente porque aplica con una intensidad diferente los principios de tratamiento de datos personales.
Aportes del texto	Las definiciones comparativas de las clases de datos que recopila el profesor Nelson Remolina permite concluir que hay un tratamiento estándar en el mundo y que al mismo tiempo el legislador colombiano transplantó la mayor parte de la normativa europea. Innovó

	en el reconocimiento de los datos personales de niños, niñas y adolescentes.
Polémicas	En la ley 1581 de 2012 ha faltado incluir el tratamiento de datos personales con fines de salud. El peligro de relativizar ciertos datos privados por hallarse en bases de datos disponibles para consulta pública.
Preguntas que suscita el texto	¿Es demasiada amplia la definición de dato público que diluiría su protección en un simple derecho de acceso a la información?
Comentario Personal	Este documento ha permitido comprender las clases de dato personal que reguló el ordenamiento jurídico colombiano para la aplicación de la LEPDP y las leyes sectoriales.
Referencia de otros autores	Warren, Samuel & Brandeis, Louis. (Diciembre, 1890). The Right to Privacy. Harvard Law Revue. The Harvard Law Review Association, Volumen 4, núm.5, 193-220 Colombia. Corte Constitucional. Sentencia T-414 de 1992. Magistrado Ponente Eduardo Montealegre Lynett. Consultada el día 04/05/16 en: http://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm Colombia. Corte Constitucional. Sentencia T-729 de 2002. Magistrado Ponente Eduardo Montealegre Lynett. Consultada el día 04/05/16 en: http://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm Colombia. Corte Constitucional. Sentencia C-748 de 2011 del 6 de octubre de 2011. Magistrado Ponente Jorge Ignacio Pretelt Chaljub.

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR :	Camilo José Puello Rincón
	GUIA N°16 de 15/05/2016
Propósito del diligenciamiento:	
Referencia Bibliográfica	Osuna Patiño, Néstor Iván (1998). <i>Capítulo Tercero. Incidencia de los valores y principios constitucionales en la determinación del objeto protegido por el recurso de amparo y la acción de tutela.</i> y <i>Capítulo cuarto: La dimensión subjetiva de los derechos fundamentales y su protección en los procesos de amparo y tutela. Y Capítulo cuarto: La dimensión subjetiva de los derechos fundamentales.</i> En: Tutela y amparo: derechos protegidos. Bogotá: Universidad Externado de Colombia.
Tema	Protección y estructura jurídica de los derechos fundamentales y
Conceptos Clave	Principios, valores, ponderación, derecho subjetivo, libertad, igualdad
Idea principal	Cuanta importancia tiene los valores y principio constitucionales en la dimensión subjetiva de los derechos fundamentales
Ideas secundarias relevantes	<p>“Haberle(...) aboga por la integración pragmática de elementos teóricos (...) Se llega así a una comprensión abierta, <i>mezclada</i> de los derechos fundamentales, que es capaz de reaccionar en contra de nuevas situaciones de peligro, y que renuncia a cierto tipo de pensamiento encasillado, de tipo escolástico”(P.208)</p> <p>“Los enunciados sobre principios fundamentales son por esencia abiertos e indeterminados, fruto de compromisos pluralistas, y permiten, por tanto, encontrar alusiones a varias teorías de derechos fundamentales”(P.209)</p> <p>Las constituciones colombiana y española no imponen una teoría material específica de los derechos fundamentales, se analizarán a continuación, en el capítulo, los valores que forman las Constituciones mencionadas.</p> <p>La concepción liberal de la libertad es entendida como el ejercicio de “ (...) voluntad individual (...) quien dicta las leyes de actuación de los individuos (...) pero a la vez el principio tiene un ámbito público, cuyo objeto es la elección común con otros y la realización</p>

de una concepción política de lo justo y lo bueno”(P.211) Así los derechos fundamentales son la “concreción jurídica de la libertad”, “(...) y se trata de una libertad *sin más*, esto es carece de relevancia para el mundo jurídico el objetivo que persiga el titular al hacer uso de ella”(P.212). “La formulación de los derechos se circunscribe por tanto a aquéllos que suponen una no interferencia en la autonomía individual”(P.213) Su debilidad reside en esta abstención, que cobija al Estado, “(...) no le corresponde ninguna obligación de aseguramiento o garantía para la realización material de la libertad proclamada mediante los derechos fundamentales”(P.214)

“La propuesta de ampliación democrática de los derechos fundamentales se originó como una primera objeción al modelo liberal-burgués (...) hoy no se concibe la posibilidad de realización de los derechos fundamentales fuera de los sistemas democráticos” (P.215) Esta propuesta es la manera que queda para permitir que el derecho y el estado conserve su legitimidad. Las causas de esta propuesta se deben a la inconsistencia jurídica de varios pilares del Estado de Derecho liberal y al deseo de los obreros, clase social generada con la revolución, de obtener el nivel de vida y derechos de la burguesía capitalista. Su sustento filosófico-jurídico es la concepción de estado social y económico las teorías keynesianas.

Capitulo cuarto: La dimensión subjetiva de los derechos fundamentales.

“Con la doctrina de los derechos públicos subjetivos, los derechos empezaban a asomar la cabeza en una tradición del derecho público básicamente estatalista, es decir, en un ambiente jurídico y político todavía hostil a una transformación profunda del orden heredado, un orden en el que el estado con su autoridad, estaba por delante de los individuos, con sus derechos” (Zagrebelsky cit. por Osuna en nota al pie de pág.239)

El derecho se asoció al término de ley, el germen del derecho público subjetivo, luego al concebirse la persona estatal como sujeto de derechos, puede hacer exigencias a sus ciudadanos quienes están atados como súbditos. “Pero, como el ciudadano carece de facultad de imponer su voluntad al Estado, y en consecuencia no puede oponer pretensiones al mismo, tales situaciones no son auténticos derechos subjetivos, sino *efectos reflejos* del derecho objetivo”(P.241)

Posteriormente se relajaría la teoría, para reconocer que puede pedir la intervención el estado en la protección de los derechos. En otros términos, mientras los derechos subjetivos privados tienen por sujetos a individuos situados en plano de igualdad y que pueden disponer libremente de las facultades que el derecho objetivo les ha conferido, los públicos se desarrollan dentro de relaciones de supremacía/subordinación (...)”(P.241)por ello “las premisas teóricas en que se fundaba la teoría de los derechos públicos subjetivos eran, en apretada síntesis las siguientes: a) concepción de a Constitución como simple ley y por tanto reducción del fundamento de la libertad a una base puramente legal, fruto de la manifestación de voluntad del Estado; b) Negación de la dimensión social o colectiva como esfera autónoma de la experiencia jurídica y absorción íntegra de esta esfera por el propio Estado; c)Distinción entre derecho privado y derecho público, concebida como distinción cualitativa entre relaciones jurídicas paritarias y relaciones jurídicas desiguales;d) Concepción de las relaciones entre el Estado y los ciudadanos como relaciones interpersonales en las cuales el individuo- Estado no sólo detenta un poder general de dominio sobre los ciudadanos, sino que también es el autor y el sujeto de las leyes, a cuya observancia como máximo, se autoobliga, sin poder ser vinculado a ello por otros, e) reconocimiento de la titularidad de los derechos públicos subjetivos al individuo, no en cuanto tal, sino como ciudadano, como miembro de la comunidad nacional aun si el ejercicio de tales derechos puede estar referido a la satisfacción de un interés personal”(P.246-247)

Posteriormente juristas intentan aclarar más la diferencia entre los efectos reflejo y los derechos subjetivos. Los primeros se renombran como *intereses legítimos* que es una coincidencia de intereses particulares con el interés general y el derecho subjetivo, sólo considera el interés particular.

	<p>La teoría de los derechos públicos subjetivos intenta actualizarse dada la importancia que se tiene como institución jurídica reconocida y como el germen de la protección de intereses jurídicos especiales para el desarrollo de la personalidad por parte del Estado</p> <p>“En efecto, el proceso seguido puede exponerse de la siguiente manera: la noción de derechos subjetivos en el ámbito del derecho privado fue tomada por la doctrina alemana del siglo XIX para caracterizar como tales a determinadas relaciones que se presentaban entre los individuos y el ente político. Posteriormente, Jellinek incluyó dentro de esta relación los derechos de libertad, excluyendo de la noción el acto de disposición autónoma de intereses que la caracteriza en el ámbito privado. Esta noción de derechos subjetivos, que se tienen en calidad de ciudadano y no en virtud de un acuerdo privado de voluntades, es la que forma parte de los actuales derechos fundamentales, y son estos derechos los que ahora tienen también vigencia en las relaciones entre particulares.”(P.260)</p>
Análisis conceptual del documento	El desarrollo teórico de los derechos fundamentales desde su concepción en la teoría liberal como derechos naturales, pasando a su positivización permite comprender los aspectos centrales en la estructura de ellos.
Aportes del texto	Las conclusiones acerca de que los derechos fundamentales son derechos subjetivos de gran tutela judicial por los intereses de la persona que protegen: libertad, igualdad, solidaridad. Al mismo tiempo un mandato de realización en mayor medida posible, por ello tiene una doble cara: derechos de abstención y derechos de prestación y participación.
Polémicas	¿Debe seguir vigente la teoría de los derechos públicos subjetivos?
Preguntas que suscita el texto	NA
Comentario Personal	NA
Referencia de otros autores	Carré de Malberg. Teoría General del Estado

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N°17 de 30/05/2016
Propósito del diligenciamiento: Comprender la teoría de la Protección Inteligente de Datos Personales o <i>Privacy By Design</i> para valorar el nivel de protección de datos personales del ordenamiento jurídico de Colombia.	
Referencia Bibliográfica	Brian Nougères, A. (2012). “La protección inteligente de los datos personales”. En: <i>Revista Internacional de Protección de Datos Personales</i> . ISSN: 2322-9705. N°1 Julio-Diciembre. Recuperado el 29/02/16 de: http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian-Nougreres_FINAL.pdf
Tema	Teoría de la protección jurídica de los datos personales
Conceptos Clave	Datos personales, privacy, principios de protección de datos personales, modelo de negocio, sistemas de información, Internet, <i>Privacy by Design</i> .
Idea principal	La teoría de la <i>Privacy by Design</i> quiere proyectar los principios jurídicos de protección de datos personales a toda la actividad empresarial de tratamiento de datos personales, esto implica que la filosofía garantista se incluya en los modelos de negocio y la infraestructura de red o sistemas de información.
Ideas secundarias	El mundo en el que vivimos hoy es un mundo en que la vigilancia se considera un

relevantes	<p>insumo imprescindible para una vida armónica en sociedad, en que se procura información acerca de los individuos por todos los medios, en que se producen perfiles de las personas según sus comportamientos, acciones que pueden llevarnos a asumir conductas discriminatorias. La ubicuidad, los nuevos paradigmas que nos inducen a compartir información, las redes sociales, la computación en la nube, son factores que han ido delineando con nuevos visos la privacidad.(P.4)</p> <p>Para preservar la privacidad se formula la <i>Privacy by design</i> que pretendió extender los principios y fundamentos de protección de datos personales a la tecnología.</p> <p>Si bien hace unos años se llegó a considerar a la privacidad como un obstáculo para la innovación y el progreso, eso ya es historia y obviar la privacidad es un grave error. La realidad es que, sin la confianza de los consumidores, las tecnologías no pueden avanzar; la privacidad está en la esencia de la democracia y se presenta como la libertad de escoger y controlar nuestra información. (P.5)</p> <p>Smartprivacy</p> <p>El término SmartPrivacy, que puede traducirse como privacidad inteligente, hace referencia a un concepto que abarca un amplio espectro de medidas de protección de datos, comprensivo de todo lo necesario para asegurar que los datos personales que están en manos de las organizaciones públicas y privadas son administrados en forma adecuada.(P.6)</p> <p>Los elementos de la PbD son: a) normas y supervisión de su cumplimiento de manera independiente, b) educación y concientización, c) transparencia y rendición de cuentas, d) auditorías y control de cumplimiento de la protección de datos personales, e) Influencia del consumidor en el mercado.</p> <p>Fundamentos de la protección de datos</p> <p>Los fundamentos de la protección de datos se pueden apreciar en: A. Consentimiento, B. Rendición de cuentas, C. Finalidad, D. Limitaciones en la recolección, E. Limitaciones en el uso, la retención y la divulgación, F. Precisión, G. Seguridad, H. Apertura, I. Acceso, J. Cumplimiento (P.7)</p> <p>¿En que consiste la teoría de la Privacy by design?</p> <p>La noción de PbD refiere tanto a una filosofía como a un enfoque por el cual la privacidad se encuentra integrada en el diseño tecnológico mismo, consistente con la arquitectura del sistema de información y con el modelo de negocios.(P.8)</p> <p>Toda la idea surge alrededor de siete principios que informan la PbD y que son marcos referenciales que pueden ser utilizados para el desarrollo de criterios de aplicación del sistema y para su verificación. (P.9)</p> <p>Los principios son: a) proactividad y no reacción, prevención y no sanción(P.9), b) privacidad como configuración predeterminada(P.10) o privacidad integrada con el diseño (P.10), c) funcionalidad plena (P.11), d) visibilidad y transparencia (P.11), e) protección de datos en todo el ciclo vital (P.11), f) visibilidad y transparencia, g) respeto por la privacidad del usuario,</p>
Análisis conceptual del documento	<p>El documento expone la tesis central del surgimiento de la Privacidad por Diseño como es el de expandir la protección jurídica a los aspectos técnicos y organizaciones, mediante la estandarización de los fundamentos de protección de datos personales en las actividades de las organizaciones.</p>

	<p>Expone las principales características de esta teoría como medida para prevenir vulneraciones de datos personales y no simplemente sancionar y castigar por el incumplimiento, dadas las consecuencias actuales que representan la información personal como fuente de generación de riqueza e innovadores productos.</p> <p>La privacidad o intimidad si puede estar junto a la innovación, la técnica y los nuevos modelos de negocio, no es simplemente un obstáculo a la consecución de los fines que se trazan los gobiernos y las empresas.</p>
Aportes del texto	Comprender que los principios sustanciales para el debido tratamiento de datos personales regulados por la Ley 1581 de 2012 sobre protección de datos personales de Colombia, son mayormente inspirados de los fundamentos de la teoría de la privacidad por diseño.
Polémicas	Las empresas de internet consideran que la privacidad es un concepto obsoleto en la actualidad porque la entrega de información personal para recibir servicios es algo común y necesario.
Preguntas que suscita el texto	NA
Comentario Personal	NA
Referencia de otros autores	EUA. Senado. <i>Commercial Privacy Bill of Rights Act of 2011</i> .

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR :	Camilo José Puello Rincón
	GUIA N° 18 de 31/05/2016
Propósito del diligenciamiento: Comprender como se entiende la criminalidad informática en Colombia a través de un enfoque criminológico de las regulaciones jurídicas en el derecho penal hasta antes de la expedición de la Ley 1273 de 2009.	
Referencia Bibliográfica	Posada Maya, R.(Agosto,2006). Aproximación a la criminalidad informática en Colombia. En: <i>Revista de derecho, comunicaciones y nuevas tecnologías</i> , núm.2, pp.13-60, Facultad de Derecho de la Universidad de los Andes. Colombia. Recuperado el 04/06/16 de: https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics86.pdf
Tema	Delitos informáticos en el ordenamiento jurídico
Conceptos Clave	Ciber-crimen, medios informáticos, daño informático, software, computación
Idea principal	Los medios tecnológicos han impacto de forma positiva, pero también en forma negativa, esto último ha generado la reacción del Estado para intentar castigar a quienes usan la tecnología para obtener beneficios perjudiciales para la sociedad, por lo cual son declarados ilícitos.
Ideas secundarias relevantes	Sin embargo, como resultado del mal uso de los avances tecnológicos, informáticos y telemáticos, es evidente el incremento de la probabilidad —estadística— de nuevos peligros (amenazas) o de la producción de lesiones graves no enteramente controlables por las ‘víctimas’, no sólo frente a la información como derecho y función pública, sino, también, frente al desarrollo adecuado de los sectores sociales e industriales más importantes. (P.14)

Amenazas que entrañan, de forma subsidiaria, la pérdida de credibilidad y confianza — *individual y colectiva*— en la seguridad que las instituciones públicas y privadas están obligadas a proveer, en la gestión informática, de los productos y servicios que desarrollan. Elementos que se deben garantizar para sostener las condiciones mínimas de interacción normal de los individuos en el moderno sistema social digital (P.15)

Adicionalmente ha ocurrido que estos delitos se cometen en varios países desde otros o su actuación comienza en uno y se extiende por varios. Esto obliga a colaborar a los Estados y hacer estándar sus regulaciones penales.

No obstante lo anterior, lo cierto es que la protección penal en la materia ni es sencilla ni homogénea a nivel internacional, y en muchos casos, la tipificación de tales conductas informáticas supone privilegiar técnicas de penalización dudosas y problemáticas que desestabilizan el complejo bloque constitucional de garantías asistido por el Derecho penal liberal.

En la realidad colombiana deben adaptarse las necesidades de criminalización de las conductas cometidas a través de medios informáticos. Al respecto se valora la utilidad real sobre la simbólica, así como la legitimidad de la penalización de dichas conductas. El fin no puede ser solamente aumentar la sensación de seguridad informática a través del “instrumento punitivo”.

La criminalidad informática es un tema complejo debido a dos factores: i) la transformación permanente de las nuevas tecnologías que hace limitada la intervención punitiva, ii) la incapacidad institucional del estado para responder a cada nueva criminalidad, en especial teniendo en cuenta el fenómeno de la aterritorialidad del internet y iii) la cifra negra de criminalidad por la falta de denuncia ante el miedo de ver afectado el prestigio social por causa de la carga simbólica negativa que representa ser víctima de un cibercrimen.

El derecho penalo sólo debe usarse cuando se agoten otras instancias legales de prevención, así su intervención estará condicionada a la subsidiariedad y necesidad de protección.

La criminalidad informática se manifiesta de dos formas: la primera es la realización de conductas punibles tradicionales que son abiertas en su verbo rector, lo cual permite que sean típicas las conductas que usen medios informáticos y la segunda son conductas que afectan directamente estos medios informáticos vulnerando su seguridad o la confianza que sobre ellos tienen las personas en su uso cotidiano. Estas conductas pueden afectar muchos bienes jurídicos y actualizar por ello varios tipos penales tradicionales o no tradicionales.

En Colombia no hay una regulación penal sobre delitos informáticos, esto implica que sea difícil juzgar estos dentro de los tipos actuales porque se presta a ambigüedades jurídicas ante la protección de bienes jurídicos específicos que ofrecen los tipos tradicionales y la poca adaptación que representarían los delitos informáticos.

“Con tal punto de partida, los delitos informáticos constituirán figuras delictivas autónomas (*delicta sui generis*), de peligro y en blanco, aplicables de forma preferente cuando se vulneren las funciones informáticas referidas a la información (*entendida como bien inmaterial público y nuevo paradigma económico*), frente a otras conductas que vulneren bienes jurídicos personales o personalísimos de forma incidental. Dicho lo cual, el problema jurídico se traslada, no solo a la cuestión de la legitimidad de las modalidades típicas necesarias para proteger dicho interés social como bien jurídico, sino también al tratamiento que se debe dar, conforme a las reglas que rigen la unidad o pluralidad de tipicidades, a las conductas que trascienden la afectación de la información y vulneren —*al tiempo*— otros bienes jurídicos como la intimidad personal” (P.22)

III. Diversas hipótesis de delitos informáticos en sentido criminológico

El autor analiza los delitos en el ordenamiento jurídico colombiano que se relacionan con medios informáticos o que tienen por objeto la afectación de estos. Para ello determina que hay cuatro clases de delitos informáticos: intrusismo, espionaje, fraude y falsedad.

Intrusismo informático: Consiste en el ingreso sin autorización a un sistema informático o red de comunicación electrónica de datos, “(...) la posibilidad fáctica – al menos un instante – de obtener servicios o disponer de la información existente y retirarla del mismo; con lo cual, se crea un peligro verificable y concreto para el titular de los bienes jurídicos” (P.24). Al respecto (P.24) afirma que es pieza clave el permiso de este último porque “es lo que permite la conexión normal al medio informático y lucrarse de manera lícita (aun cuando sea el mismo prestador del servicio sin legitimidad, arguyendo razones de verificación).” (P.23)

Se excluyen medidas que no tengan como fin *limitar el acceso* sino *prevenir el ingreso* al sistema informático o página web. También menciona que pueden existir medidas de seguridad que carecen de la idoneidad suficiente para proteger el sistema informático conforme a lo que dictaminaría un técnico experto o al estándar de la industria en la materia. Por esta falta al deber de cuidado el autor argumenta la posibilidad de que haya un tipo penal que castigue la *omisión del control debido de la gestión de seguridad informática* dado que “(...) la sola tenencia legítima de datos o de información de terceros (bancos de datos financieros, contables, etc.) constituye una modalidad de *actividad peligrosa*” (P.27) porque están fuera del control directo del titular de esa información.

Pueden excluirse los “ingresos inocentes”, aquellos que ocurren de manera incidental o bajo error del mismo sistema y el usuario permanece allí sin percatarse de que es una zona no autorizada o sin intención de provocar una alteración en el sistema. Aunque por el *mero peligro* que viene rodeando al tipo penal probablemente será típica su conducta pero excluyente de responsabilidad.

“Adicionalmente, todo indica que el tipo penal descrito en el art. 195 constituye una cláusula general, pues, como se advirtió, paradójicamente el legislador no exige que el ‘intruso’ actúe bajo el influjo de elementos subjetivos especiales orientados a obtener datos informáticos, dañar, lucrarse o interferir el sistema al que se ha conectado. Con lo cual se promueve jurídicamente, en principio, la sanción penal de una serie de comportamientos de intrusismo directo *inofensivo* que normalmente no deberían castigarse por la vía penal —*pero sí administrativa*—; como sucede con el denominado “*hacking blanco o Joyriding*”⁴², en el cual el intruso carece de intención de lesionar, lucrarse o causar daño en provecho propio o de terceros, dado que despliega la conducta con el fin de ocupar la red por curiosidad o desafío intelectual, a la par que señala la insuficiencia de las medidas de seguridad que posee el sistema. Ello, con independencia de la responsabilidad que se pueda derivar de los hechos, como consecuencia de los daños causados al hacer obsoletas las medidas de seguridad previamente dispuestas por el titular del sistema, al bloquear los sistemas o generar borrados accidentales en los datos o información informatizada contenida en los medios.” (P.28)

Espionaje informático

“Por tal modalidad criminal deben entenderse aquellas actividades dirigidas a obtener, captar y desarrollar sin autorización datos, comunicaciones, programas, licencias, imágenes y sonidos almacenados en ficheros o bases de datos públicos o privados, donde se acumula y procesa información confidencial, exclusiva y valiosa protegida. Sobre el particular, los supuestos se deben diferenciar por virtud de la protección penal que se otorga a los distintos bienes jurídicos involucrados: *la intimidad, el orden económico social y la seguridad del Estado.*”

	<p><i>Fraude informático</i></p> <p>Esta modalidad delictiva, también conocida como “<i>Fraud by computer manipulation</i>”, se puede desarrollar a través de manipulaciones a los usuarios de la Internet, a los programas de funcionamiento de sistemas informáticos y telemáticos o a los contenidos de bases de datos, afectando de este modo el almacenamiento, procesamiento o transferencia de datos o información informatizada⁶⁸, el patrimonio económico o la administración pública. (P.42)</p> <p><i>Falsedad informática</i></p> <p>“(…)[C]onsiste consiste en el uso, adulteración, modificación, creación por imitación total o parcial, destrucción u ocultamiento temporal o definitivo de documentos electrónicos públicos o privados por medios informáticos, a condición de que los mismos puedan servir de prueba. Conductas que están dirigidas a simular su veracidad, legitimidad, oponibilidad y autenticidad en el tráfico documental, en el marco de una clara violación a la fe pública (identidad probatoria de los datos o informaciones).” (P.46)</p>
Análisis conceptual del documento	El derecho penal tiene ante los delitos informáticos un gran reto de regulación y eficacia jurídica. De regulación en cuanto a que los tipos penales en la mayor parte pueden quedar desactualizados ante el avance, pero el hecho de establecerlos como tipos en blanco puede someterlos a ambigüedades riesgosas para el principio de legalidad y también al hecho de que puedan vulnerar el principio de culpabilidad si se establecen como tipos de peligro en consideración de llevar el concepto de actividad riesgosa al derecho penal de la actividad informática.
Aportes del texto	El análisis criminológico de la incidencia del Internet y las nuevas tecnologías en la comisión de delitos en Colombia hasta antes de la ley 1273 de 2009. En esta última se ven varias críticas y propuestas formuladas en este artículo.
Polémicas	NA
Preguntas que suscita el texto	NA
Comentario Personal	NA
Referencia de otros autores	<p>Bekerman, Jorge M.: Informática: su regulación jurídica internacional “vis-á-vis” la brecha tecnológica, en: El derecho y las nuevas tecnologías. Contexto económico, social y cultural. AA.VV., separata, Separata de Revista del Derecho industrial, No. 33, Buenos aires, Depalma, 1990.</p> <p>Castro Ospina, Sandra Jeannette: Delitos Informáticos: La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano, Madrid, DelitosInformaticos.com, 15.07.2002. http://www.delitosinformaticos.com/delitos/colombia.shtml.</p> <p>Chiaravalloti, Alicia; Levene, Ricardo. Introducción a los delitos informáticos, tipos y legislación (Publicado en el VI Congreso Latinoamericano en 1998, en Colonia, Uruguay. Publicado en La Ley, Nros. 202 del 23 de Octubre de 1998 y 215 del 11 de Noviembre de 1998, Argentina.) (En línea) Madrid, DelitosInformaticos.com, 02.12.2002. http://delitosinformaticos.com/delitos/delitosinformaticos.shtml</p>

	<p>Consejo de Europa: Convención sobre el Cibercrimen, Budapest 23 de Noviembre de 2001, serie de tratados europeos Núm. 185, preámbulo, En: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.</p> <p>González Rus, Juan José. Protección penal de sistemas, elementos, datos, documentos y programas informáticos (Revista Electrónica de Ciencia Penal y Criminología RECPC, 01-14-1999) (en línea). Granada, CRIMINET, Web de Derecho Penal y Criminología, 2004. http://criminnet.ugr.es/recpc/recpc_01-14.html.</p>
--	--

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N°18 de07/06/2016
Propósito del diligenciamiento: Obtener el conocimiento y comprensión de los criterios para determinar el nivel de protección adecuado de datos personales que usa la Union Europea para calificar a un país no miembro.	
Referencia Bibliográfica	<p>Unión Europea. Comisión Europea. (26 de junio de 1997) Documento de trabajo N° WP4 “Primeras orientaciones sobre la transferencia de datos personales a países terceros Posibles formas de evaluar la adecuación”.</p> <p>Recuperado el 8 de junio de 2016 de, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_es.pdf</p>
Tema	Criterios para evaluar el nivel de adecuación normativa de un estado sobre protección de datos personales.
Conceptos Clave	Nivel de protección adecuada, transferencia internacional de datos personales,
Idea principal	“Este documento (...) pretende centrarse en la cuestión de evaluar la <i>adecuación</i> en el sentido de los apartados 1 y 2 del artículo 25”(P.2)
Ideas secundarias relevantes	<p>Se busca racionalizar los procesos de evaluación del nivel adecuado de protección de datos personales y de las transferencias adecuadas debido a la gran cantidad de solicitudes. Dos maneras son las <i>listas blancas</i> que definen un permiso provisional, que no reconocimiento de nivel adecuado, para hacer la transferencia y el <i>análisis específico de riesgos</i> que se concentra en transferencias específicas de datos personales.</p> <p>Por nivel adecuado se entiende que es “(...) una combinación de derechos para el sujeto de los datos y de obligaciones para aquellos que procesan los datos o que ejercen un control sobre dicho tratamiento.” (P.5) También se requiere que pueden ejercerse los derechos y obligaciones mediante unos mecanismos específicos diseñados para ello.</p>

El análisis se realiza a partir de la Directiva 94/46/CE y toma en cuenta tres aspectos: principios de protección de datos, requisitos de aplicación, requisitos procedimentales.

Sobre los principios y su contenido afirma lo siguiente: i) principio de limitación del propósito (los datos deben tratarse con un propósito específico y conocido por el titular del dato), ii) la calidad de los datos y principio de proporcionalidad (significa que los datos deben ser preciso, integros, actualizados y proporcionales a la finalidad), iii) Principio de transparencia (asegura que los individuos sean informados del controlador de los datos, de los propósitos de su información, iv) principio de seguridad (el controlador debe ofrecer unas medidas técnicas y organizacionales pertinentes para evitar los riesgos del presente tratamiento), v) derechos de acceso, rectificación y oposición (el sujeto de los datos deberá tener derecho a copia de los datos relativos a él que se tengan, pudiendo solicitar que se corrijan errores u oponiéndose al tratamiento), vi) restricciones a la transferencia sucesivas a otros países terceros (prohibir que se transmitan a países que no tengan el nivel adecuado de protección).

Adicionalmente se debe tener el consentimiento explícito para los datos sensibles, marketing directo y la decisión individual automatizada.

También existe un amplio acuerdo acerca de que un sistema “de control externo” en forma de una autoridad independiente es una característica necesaria para un sistema de aplicación de la protección de datos.

“1) Proporcionar un buen nivel de cumplimiento de las normas. (Ningún sistema puede garantizar un cumplimiento al 100%, pero hay sistemas mejores que otros). Un buen sistema se caracteriza generalmente por un elevado nivel de concienciación entre los controladores de datos respecto de sus obligaciones, y entre los sujetos de los datos respecto de sus derechos y su forma de ejercicio. La existencia de sanciones efectivas y disuasorias es importante para garantizar el respeto por las normas, así como los sistemas de comprobación directa por parte de las autoridades, auditores o funcionarios independientes responsables de la protección de datos.

	<p>2) Proporcionar apoyo y ayuda a los sujetos de datos individuales en el ejercicio de sus derechos. Los individuos deberán ser capaces de ejercer sus derechos de forma rápida y eficaz, y sin costes prohibitivos. Para ello deberá existir algún tipo de mecanismo institucional que permita una investigación independiente de las denuncias.</p> <p>3) Proporcionar una reparación adecuada a las partes perjudicadas cuando no se cumplan las normas. Esto es un elemento clave que debe contar con un sistema de arbitraje independiente que permita pagar una compensación e imponer sanciones cuando sea oportuno.” (P.8)</p>
Análisis conceptual del documento	Este documento da unos lineamientos bastante básicos acerca de lo que se entiende por nivel adecuado de protección de datos personales. Su énfasis es en los principios generales, falta desarrollar la parte de los mecanismos y procedimientos, no da muchos detalles y lo deja a la iniciativa de los Estados miembros.
Aportes del texto	La relación intrínseca que hay entre los principios y las herramientas jurídicas que permitan desarrollarlos mejor para cumplir con la aplicación práctica de ellos que son los derechos de los titulares.
Polémicas	NA
Preguntas que suscita el texto	NA
Comentario Personal	NA
Referencia de otros autores	NA

Análisis de guía análisis jurisprudencial

GUIA DE ANALISIS JURISPRUDENCIAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 01 de 03/05/2016
Propósito del diligenciamiento: Obtener la información pertinente sobre la posición jurisprudencial de la Corte Constitucional acerca del análisis de constitucionalidad de la ley estatutaria de protección de datos personales. De esta manera se va a identificar el desarrollo de la línea jurisprudencial	
Identificación de la Providencia	
Corporación y Sala Sentencia N° Medio de Acción Fecha Magistrado Ponente	Corte Constitucional colombiana C-748 Control de constitucionalidad previo y oficioso de proyectos de ley sobre derechos fundamentales según art. 241-8 constitucional 6 de octubre de 2011

Magistrados Integrantes Sala Plena de la Corte	Jorge Ignacio Pretelt Chaljub Juan Carlos Henao Pérez –quien la preside, María Victoria Calle Correa, Mauricio González Cuervo, Gabriel Eduardo Mendoza Martelo, Jorge Iván Palacio Palacio, Nilson Pinilla Pinilla, Jorge, Humberto Antonio Sierra Porto y Luis Ernesto Vargas Silva
--	--

1. Intervenciones

Dentro del proceso se presentaron intervenciones de las siguientes personas y entidades: el Ministerio de Industria, Comercio y Turismo, la Secretaría Jurídica de la Presidencia de la República, la Defensoría del Pueblo, los ciudadanos Juanita Durán Vélez, Santiago Diazgranados Mesa, Alejandro Salas Pretelt, Rolfe Hernando González Sosa y María Lorena Flórez Rojas, la Universidad de los Andes, la Fundación para la Libertad de Prensa (FLP), Computec S.A. – Datacrédito, la Asociación Colombiana de Empresas de Medicina Integral (ACEMI), la Asociación Bancaria de Colombia y Entidades Financieras de Colombia (ASOBANCARIA).

La Sala hará referencia al contenido de cada una de las intervenciones al realizar el análisis de constitucionalidad tanto formal como material de cada una de las disposiciones del proyecto de ley bajo estudio.

2. Concepto del Procurador General de la Nación

Se consignarán las posiciones más importantes a juicio del autor de esta ficha de análisis.

- El proyecto de ley cumple con todas las formalidades requeridas para que sea una ley estatutaria de la República.
- Sostiene que las excepciones consagradas al principio de prohibición de tratar datos sensibles deben pedir la autorización a los titulares del dato personal.
- Quienes pueden acceder sin consentimiento en los casos de urgencia médica manifiesta deben ser solamente los médicos y enfermeras tratantes.
- El inciso 2° del artículo 10 considera que debe ser declarado inexecutable debido a que a través del permiso concedido por este artículo se abre la posibilidad de “limpiar” aquellos tratamientos de datos obtenidos siempre que posteriormente cumpla la ley.

3. Consideraciones de la Corte

A. Metodología previa al análisis del proyecto

“La revisión integral del proyecto de ley estatutaria se desarrollará de la siguiente manera. **En primer lugar**, y de manera previa al estudio de constitucionalidad, la Sala hará una referencia al origen histórico y el alcance del derecho fundamental al habeas data. **En segundo lugar**, determinará cuál fue el modelo de regulación adoptada por el legislador estatutario y sus implicaciones en el análisis de constitucionalidad de las disposiciones del Proyecto. Establecido el marco general de protección de datos en Colombia, la Corporación realizará el análisis tanto formal como material del articulado del proyecto”

A primera vista del presente proyecto de ley “(...)indica que su objetivo principal es regular de manera general las garantías del derecho fundamental a la protección de los datos personales, derecho que en la jurisprudencia constitucional ha sido con frecuencia denominado derecho al habeas data y en algunas oportunidades derecho a la autodeterminación informática o informativa. Para determinar si, en efecto,

el proyecto regula al menos algunos de los contenidos mínimos de este derecho, a continuación la Sala examinará su origen y alcance:

B. Ratio decidendi

“El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios [20] que informan el proceso de administración de bases de datos personales”.

“De conformidad con la jurisprudencia de esta Corporación, dentro de las prerrogativas –contenidos mínimos- que se desprenden de este derecho encontramos por lo menos las siguientes: (i) el derecho de las personas a conocer –acceso- la información que sobre ellas está recogida en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de se provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificadas o corregidas, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa.”

La regulación de los procedimientos para hacer efectivos los derechos fundamentales puede incluirse o no en la ley estatutaria del derecho, sin embargo no es obligación del legislador porque no hace parte del núcleo esencial, cuyos elementos se mencionan antes. “Ahora bien, tales herramientas pueden ser tanto de naturaleza judicial como administrativa, es decir, el literal a) hace referencia (i) tanto a acciones o recursos que permiten reclamar la satisfacción de un derecho ante un juez y que implican la existencia de un proceso, (ii) como a mecanismos administrativos tales como órganos de vigilancia y control y procesos administrativos dirigidos a resolver controversias relacionadas con la realización de los derechos fundamentales.”

“El artículo 3 del proyecto define las base de datos de una manera muy amplia como el “[c]onjunto organizado de datos personales que sea objeto de Tratamiento”. El tratamiento, por su parte, es definido como “[c]ualquier operación o conjunto de operaciones sobre datos personales, tales como recolección, almacenamiento, uso, circulación o supresión”.

El literal a) ofrece tres contenidos normativos: (i) señala que uno de los casos exceptuados de la reglas del proyecto es el de “las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico”. (ii) A continuación, indica que “cuando estas bases de datos vayan a ser suministradas a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización.” Por último, (iii) precisa que en este último caso, es decir, cuando los datos son suministrados a un tercero, el respectivo responsable o encargado de las bases de datos y archivos quedará sujeto a las disposiciones de la ley.

Los criterios de (i) definición de los fines y medios del tratamiento del dato personal y (ii) existencia de delegación, también resultan útiles en nuestro caso para establecer la diferencia entre responsable y encargado. Ciertamente, el concepto “decidir sobre el tratamiento” empleado por el literal e) parece coincidir con la posibilidad de definir –jurídica y materialmente- los fines y medios del tratamiento. Usualmente, como reconocen varias legislaciones, el responsable es el propietario de la base de datos; sin embargo, con el fin de no limitar la exigibilidad de las obligaciones que se desprenden del habeas data, la Sala observa que la definición del proyecto de ley es amplia y no se restringe a dicha hipótesis. Así, el concepto de responsable puede cobijar tanto a la fuente como al usuario, en los casos en los que

dichos agentes tengan la posibilidad de decidir sobre las finalidades del tratamiento y los medios empleados para el efecto, por ejemplo, para ponerlo en circulación o usarlo de alguna manera.

En la sentencia C-1011 de 2008[198], se señaló que en la administración de datos personales es posible identificar varias etapas, cuya diferenciación permite adscribir determinados niveles de responsabilidad a los sujetos que participan de él. (...)

En esa línea, lo importante para una verdadera garantía del derecho al habeas data, es que se pueda establecer de manera clara la responsabilidad de cada sujeto o agente en el evento en que el titular del dato decida ejercer sus derechos. Cuando dicha determinación no exista o resulte difícil llegar a ella, las autoridades correspondientes habrán de presumir la responsabilidad solidaria de todos, aspecto éste sobre el que guarda silencio el proyecto de ley y que la Corte debe afirmar como una forma de hacer efectiva la protección a la que se refiere el artículo 15 de la Carta”.

(...)[P]uede entonces deducirse: (i) los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo, expreso e informado del titular. Es decir, 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 y (iii) el principio de libertad no sólo implica el consentimiento previo a la recolección del dato, sino que dentro de éste se entiende incluida la posibilidad de retirar el consentimiento y de limitar el plazo de su validez.

“(...) [T]al como lo estableció la Corte en la Sentencia C-1011 de 2008, la naturaleza de las facultades atribuidas a la Superintendencia –a través de la Delegatura-, *“caen dentro del ámbito de las funciones de policía administrativa que corresponden a esos órganos técnicos adscritos al ejecutivo (Art. 115 C.P.), en tanto expresión de la potestad de dirección e intervención del Estado en la economía (Art.334), y de intervención reforzada del Gobierno en las actividades financiera, bursátiles y aseguradoras (Art. 335 C.P.).”*

“(...)la asignación de facultades (...) a la Superintendencia de Industria y Comercio, *“no puede interpretarse como el desplazamiento o la reasignación de competencias que constitucional o legalmente le han sido atribuidas a otros órganos institucionales de control(...), órganos como la Defensoría del Pueblo, por ejemplo, conservan a plenitud sus competencias constitucionales (Art. 282 C.P.) y legales (Ley 24 de 1992) que le imponen velar por la promoción, ejercicio y divulgación de los derechos humanos, y por ende, del derecho fundamental al hábeas data”*.

En relación con el inciso segundo, la Sala encuentra que hace un reenvío al Código Contencioso Administrativo en lo que hace al procedimiento que debe aplicarse para la imposición de las sanciones.

El artículo 14 del proyecto de ley regula el mecanismo de la consulta al señalar: (i) que los titulares o sus causahabientes podrán consultar la información personal del titular que repose en cualquier base de datos pública o privada, (ii) responsables y encargados del tratamiento deben suministrar al titular toda la información contenida en la base de datos bien porque se tenga un registro individual o exista alguna asociada a su identificación, (iii) el responsable y el encargado del tratamiento deben tener algún medio habilitado para que la consulta se pueda realizar, el cual debe permitir dejar prueba de ello, (iv) la consulta se debe resolver en un término máximo de 10 días hábiles a partir de la fecha de recibo de la solicitud y (v) en el evento de no poder responderse en ese término, se le debe informar al titular sobre

las razones. De todas maneras la respuesta la debe recibir dentro de los 5 días siguientes al vencimiento del primer plazo.

En ese sentido, el legislador estatutario al regular de forma general la protección del dato personal, estaba facultado para señalar los términos en que los responsables y encargados del tratamiento del dato, públicos y privados, deben responder las consultas o peticiones que les eleve el titular del dato o sus causahabientes, con el fin de hacer exigibles entre otros, el derecho a conocer qué datos personales tiene un determinado bancos de datos y la forma como éstos son manejados. Compatible con esto, los artículos 17, literal k) y 18 literal f) del proyecto, establecen como uno de los deberes del responsable y encargado del tratamiento del dato, el de adoptar un manual interno de políticas y procedimiento especialmente para la atención de las consultas y reclamos por parte de los titulares.

C. Obiter Dictas

El derecho al habeas data tiene su origen en el derecho a la intimidad que reconocen múltiples declaraciones de derechos humanos: art. 12 de la Declaración de 1948 de la ONU o en el art.17 del Pacto de los Derechos Civiles de 1966 o en la Convención Americana de los Derechos de 1948 en su art.11.

En Europa se inicia el camino para reconocer el habeas data como derecho fundamental autónomo a partir de la incidencia que comienza a tener la tecnología en el derecho a la intimidad.

“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.”

La configuración de la autodeterminación informativa como derecho autónomo culmina con la Carta de los Derechos Fundamentales de la Unión Europea de 1999, cuyo artículo 8 reconoce explícitamente el derecho de toda persona a “la protección de los datos de carácter personal que la conciernan” y dispone que “[e]stos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley.” Además, indica que “[t]oda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación”, y señala que la verificación del cumplimiento de estas garantías debe encargarse en cada estado a un órgano independiente.

En Colombia se encuentra el artículo 15 de la Constitución de 1991, vigente en el país, y algunas leyes sobre temas específicos de privacidad de la información personal

En la jurisprudencia constitucional, el derecho al habeas data fue primero interpretado **como una garantía del derecho a la intimidad**, de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir.

A partir de 1995, surge una tercera línea interpretativa que apunta al habeas data como **un derecho autónomo** (...) según la sentencia SU-082 de 1995[15], el núcleo del derecho al habeas data está compuesto por la autodeterminación informática y la libertad –incluida la libertad económica

Nota 1º: “*Debe tenerse en cuenta que la denominación ‘hábeas data’ no ha sido la única utilizada por la jurisprudencia para identificar las facultades del sujeto concernido respecto de las bases de datos. Así, durante el desarrollo del concepto en las decisiones de la Corte se han usado las expresiones de*

*‘autodeterminación informática’ o ‘autodeterminación informativa’. En todo caso, estas tres definiciones refieren a la misma realidad jurídica, por lo que no ofrecen mayores dificultades en su uso alternativo. Sin embargo, ante la necesidad de contar con una descripción uniforme y habida cuenta el uso extendido del término en el ámbito del derecho constitucional colombiano, esta sentencia utilizará el vocablo *habeas data* con el fin de nombrar el derecho que tienen todas las personas a ejercer las facultades de conocimiento, actualización y rectificación de la información personal contenida en bases de datos.”*

Lo primero que advierte la Sala, al igual que lo hicieron algunas intervenciones, es que a diferencia de lo que ocurrió en la Ley 1266, el legislador recurrió en esta oportunidad a conceptos propios del modelo europeo para referirse a las personas vinculadas al tratamiento del dato personal. Para algunos intervinientes este hecho no sólo es un problema de técnica legislativa (en la medida en que conduce a la coexistencia de dos modelos normativos que tienen por objeto hacer una regulación completa de una materia tan importante como el *habeas data*, pero con una terminología diversa), sino un problema constitucional, porque esa diferencia en los vocablos conlleva la dilución de la responsabilidad de quienes participan en el tratamiento del dato.

Por su parte, **la Directiva 95/46/CE**, sistematiza las directrices del manejo de los datos y reconoce que tales disposiciones se encuentran encaminadas a *“la protección de las libertades y de los derechos fundamentales a las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de datos personales”* (artículo 1). El instrumento divide los principios en dos categorías: (i) los relativos a la calidad del dato y (ii) los concernientes a la legitimidad en el manejo de la información.

En relación con los primeros dispone (artículo 6) que los datos personales sean: *“(i) Tratados de manera leal y lícita, (ii) Recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas, (iii) Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente, (iv) Exactos y, cuando sea necesario, actualizados; deberán tomarse las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificadas, (v) Conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un periodo más largo al mencionado, con fines históricos, estadísticos o científicos.”*

En cuanto a los segundos, la Directiva establece que el manejo de los datos sólo puede realizarse con el consentimiento inequívoco del titular y cuando es necesario : (i) *“para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales.”*, (ii) *“para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento”*, (iii) *“para proteger el interés vital del interesado”*, (iv) *para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos”* y (v) *para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 de la presente directiva”*.

Precisamente, dentro de esa idea de garantía institucional del derecho al habeas data y con fundamento en los estándares internacionales, se han creado instituciones **autónomas e independientes** para la protección de los datos personales, entes centralizados que solo pueden fijar políticas en clave de protección del derecho al habeas data y con poder coercitivo suficiente para lograr su efectiva protección, sin injerencias por parte de autoridades o personas que puedan limitar su correcta funcionalidad, en especial frente a los agentes privados que tienen hoy una alta capacidad para el manejo de datos personales. Obviamente en lo público, la automatización de datos se ha convertido en algo esencial para el cumplimiento de las funciones asignadas al Estado, por ejemplo, en materias como la salud y la hacienda, por señalar sólo algunas que requieren por parte del ciudadano de mecanismos de protección claros, por entes públicos y privadas que están tratando sus datos.

En ese orden, tanto los responsables como los encargados del tratamiento están obligados a observar esos parámetros que en términos generales se pueden resumir de la siguiente manera: (i) la respuesta debe ser de fondo, es decir, no puede evadirse el objeto de la petición, (ii) que de forma completa y clara se respondan a los interrogantes planteados por el solicitante, (iii) oportuna, asunto que obliga a respetar los términos fijados en la norma acusada.

D. Definiciones dogmáticas

- **Habeas Data:** “(...) es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales”.
- **Ámbito de aplicación de la ley:** Se aplicará a los tratamientos realizados sobre bases de datos, entendidos como “(...) los archivos –para efectos exclusivamente del proyecto-, en tanto son (i) depósitos ordenados de datos, incluidos datos personales, y (ii) suponen, como mínimo, que los datos han sido recolectados, almacenados y, eventualmente, usados –modalidades de tratamiento, son una especie de base de datos que contiene datos personales susceptibles de ser tratados y, en consecuencia, serán cobijados por la ley una vez entre en vigencia.”
- **Dato personal:** Características “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.”
- **Principio de autorización para la legalidad del tratamiento:** “(...) la autorización debe ser suministrada, en una etapa anterior a la incorporación del dato. Así por ejemplo, en la Sentencia T-022 de 1993^[233], se dijo que la veracidad del dato no implica que el Responsable del Tratamiento no tenga el deber de obtener una autorización anterior. En igual sentido, la Sentencia T-592 de 2003^[234] dijo que el derecho al *habeas data* resulta afectado cuando los administradores de la información recogen y divulgan hábitos de pago sin el consentimiento de su titular. La Corte expresó que el consentimiento **previo** del titular de la información sobre el registro de sus datos económicos “en los procesos informáticos, aunado a la necesidad de que aquel cuente con oportunidades reales para ejercer sus facultades de rectificación y actualización durante las diversas etapas de dicho proceso, resultan esenciales para salvaguardar su derecho a la autodeterminación informática.”

B. Obiter Dictas

5. De la Segunda Instancia

NO APLICA

- a) Consideraciones respecto al problema jurídico
- b) Tesis de la Corporación
- c) Fundamentos de la Tesis de la Corporación
- d) Salvamentos de voto

6. Análisis Crítico

- a) Identificación de precedentes
Sentencias T-414 de 1992, Sentencia C-1011 de 2008, T-592 de 2003, SU-082 de 1995 y T-729 de 2002.
- b) Reglas aplicadas

La equivalencia entre los términos habeas data y autodeterminación informativa, los derechos que hacen parte del artículo 15, destacando el habeas data como independiente, la definición de datos personales: Sentencia T-729 de 2002.

Principios de administración o tratamiento de datos personales que deben cumplirse (sentencia T-729 de 2002)

- c) Comentario
Esta sentencia es un compendio bastante rico de todo el desarrollo jurisprudencial que ha hecho la Corte Constitucional sobre el derecho fundamental al habeas data: el contenido esencial, los derechos que lo integran, los principios indispensables para evitar la vulneración, los tipos de datos personales, la forma de tratamiento, ejercicio de los mecanismos de protección.

GUIA DE ANALISIS JURISPRUDENCIAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 02 de 03/05/2016
Propósito del diligenciamiento: Obtener la información pertinente sobre la posición jurisprudencial de la Corte Constitucional acerca del análisis de constitucionalidad de la ley estatutaria de protección de datos personales. De esta manera se va a identificar el desarrollo de la línea jurisprudencial	
Identificación de la Providencia	
Corporación y Sala Sentencia N° Medio de Acción	Corte Constitucional colombiana T-414 Control de constitucionalidad concreto a través de la acción de tutela
Fecha Magistrado Ponente	16 de junio de 1992 Ciro Angarita Baron

1. Posición jurídica de la parte actora

a. Hechos Relevantes:

- El peticionario figura como deudor moroso del Banco de Bogotá en la Central de Información de la Asociación Bancaria de Colombia por razón de un crédito respaldado con un pagaré, el cual se vencía inicialmente el 14 de Julio de 1981 y fue prorrogado hasta el 14

- de Noviembre de 1981.
 - Por sentencia debidamente ejecutoriada, el Juzgado Décimo Sexto Civil del Circuito de Bogotá declaró prescrita la obligación del peticionario, el 27 de Abril de 1987.
 - Tanto el 8 de Noviembre de 1988 como el 18 de Junio de 1991 el señor Argüelles, personalmente y por intermedio de apoderado, solicitó a la Asociación Bancaria que lo retirara de la lista de deudores morosos.
 - Mediante oficio 004407 del 26 de Junio de 1991 la Asociación Bancaria se negó rotundamente a acceder a su solicitud.
 - El 24 de Junio de 1991 el peticionario elevó igual solicitud al Banco de Bogotá, el cual la rechazó verbalmente.
 - En virtud de todo lo anterior, el señor Argüelles aparece como deudor moroso en el banco de datos de la Asociación Bancaria cuatro años después de ejecutoriada la sentencia que declaró extinguida su obligación.
- b. Argumentos Jurídicos del Accionante: Con lo acontecido se han vulnerado el derecho al buen nombre y al habeas data de la persona al mantenerlo en la base de datos como moroso cuando la deuda fue declarada prescrita.
- c. Pretensiones:
- a) Que se le retire de la lista de deudores morosos y que se actualice y rectifique la información que sobre él existe en el banco de datos de la Asociación Bancaria.
 - b) Que se ordene a la Asociación y/o Banco de Bogotá a indemnizar el daño emergente ocasionado al peticionario.
 - c) Que se condene a los responsables en costas

2. Posición jurídica del demandado

- a. Argumentos jurídicos del Demandado: No se encontraron argumentos del demandado.

3. Planteamiento del problema jurídico

¿Es constitucional mantener el registro negativo de una persona a quien se le declaró a su favor la prescripción de una obligación que debía?

4. Fallo de Instancia

- a. Consideraciones: No es procedente la acción de tutela contra la ASOBANCARIA porque la sanción fue impuesta por el Banco de Bogotá, quien debió proceder al borrado de la información en cumplimiento de la sentencia. Sin embargo no es procedente la acción de tutela porque las pretensiones pueden tramitarse por la acción ordinaria de reparación ante la SuperBancaria o mediante proceso ordinario.
- b. Decisión de Primera Instancia: Denegó la tutela del derecho al habeas data porque hay otros mecanismos para que le reparen por los perjuicios causados

5. De la Segunda Instancia

- a. Consideraciones respecto al problema jurídico

No se mostraron las consideraciones en la sentencia.

- b. Tesis de la Corporación

Fue confirmada la decisión de improcedencia de la tutela porque cuenta con otros medios de protección del quejoso.

- c. Fundamentos de la Tesis de la Corporación

a.- Ciertamente el derecho fundamental consagrado en el Art. 15 de la Constitución puede ser protegido con la tutela.

b.- Pero, en virtud del "principio de definitividad" al" quejoso le queda alguna acción o recurso como es la de acudir a la Superintendencia Bancaria -Sección Bancos- para que revise la actuación del Banco e imponga la correspondiente sanción o interponer los respectivos recursos administrativos, si a ello hubiere lugar.

c. -Por tanto, no procede la tutela.

6. Revisión de tutela

a. Consideraciones de la Corte

La Corte solicitó un informe a la Superintendencia Bancaria para conocer la forma como ejerce control sobre los bancos de datos financieros y crediticios, en el caso concreto, si conoció acerca de la renuencia del Banco de Bogotá a cumplir la sentencia que declara prescrita la obligación y ordena sacar de la lista de deudor moroso y si existe un medio de defensa llamado acción ordinaria de reparación ante esa entidad. Respecto a lo cual responde que no tiene competencia para ejercer control sobre los bancos de datos y que cuando las personas elevan queja ante la entidad ellos piden informe al banco, cuando comprueban que la información transmitida al banco de datos es fidedigna archivan la queja y si no le ordenan que la corrija; en el caso de las conocer la renuencia al cumplimiento de la sentencia, afirman que el procedimiento es independiente a las actuaciones que adelantan ellos; respecto a la acción ordinaria de reparación, afirma que no existe en el ordenamiento. La Corte Constitucional concluye que no hay otro mecanismo idóneo, por lo cual la acción de tutela es procedente, ya que garantiza la efectividad de los derechos fundamentales consagrados en la Constitución.

(...)

“Como bien lo destaca el profesor Vittorio Frosini, la posibilidad de acumular informaciones en cantidad ilimitada, de confrontarlas y agregarlas entre sí, de hacerle un seguimiento en una memoria indefectible, de objetivizarlas y transmitir las 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.

Como necesario contrapeso, este nuevo poder ha engendrado la libertad informática. Consiste ella 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. Es, como se ve, una nueva dimensión social de la libertad individual diversa, y por razón de las circunstancias que explican su aparición, de otras clásicas manifestaciones de la libertad.

Por su peculiar naturaleza, esta libertad ha sido reconocida en las legislaciones de Estados de democracia liberal mediante estatutos jurídicos especiales, los cuales, establecen nuevos derechos e instituciones de control. En España, Portugal, y Brasil, por ejemplo, tanto la libertad informática como el habeas data han recibido el honor de una clara y explícita consagración constitucional.”

5.- *La cárcel del alma y el derecho al olvido*

(...)

El encarcelamiento del alma en la sociedad contemporánea, dominada por la imagen, la información y el conocimiento, ha demostrado ser un mecanismo más expedito para el control social que el tradicional encarcelamiento del cuerpo.

(...)

Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de "personas virtuales" que afecten negativamente a sus titulares, vale decir, a las personas reales.

(...)

De otra parte, es bien sabido que las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia después de algún tiempo tales personas son titulares de un verdadero derecho al olvido.

6.- Creciente informatización social e insuficiente protección jurídica

De otra parte, la presencia de la informática en la sociedad colombiana se percibe también tanto a través de normas de carácter fundamentalmente técnico sobre la utilización de sistemas de información, equipos y servicios de procesamiento de datos como sobre la formulación y aplicación de políticas en materia de sistemas de información y del servicio de transmisión o recepción de información codificada (datos) entre equipos informáticos.

(...)

Ante esta creciente informatización de la sociedad colombiana en distintas ocasiones y foros se ha puesto de presente la carencia de instrumentos adecuados en el ordenamiento nacional para proteger la libertad de los ciudadanos contra el uso abusivo de las nuevas tecnologías de información.

7.- Uso responsable de la Informática

(...)

Igualmente y con mayor razón, a los titulares o empresarios de servicios tecnológicos y en particular de tecnologías de información, la naturaleza de su materia prima, vale decir, el dato, impone una diligencia especial en guarda del respeto a la dignidad humana sin que sea óbice el que existan o no relaciones patrimoniales que configuren propiedad. Es natural que esta diligencia sea mayor cuando se trata de actividades empresariales lucrativas que crean, ingentes riesgos de vulnerar la libertad o la honra de las personas.

7. Análisis Crítico

- a) Identificación de precedentes No aplica
- b) Reglas aplicadas

La formulación del derecho al olvido que fija el principio de caducidad del dato en datos negativos sobre la persona, pese a que sean verdad, no pueden durar mucho tiempo.

- c) Comentario

Esta sentencia fue la primera que inició el estudio jurisprudencial del derecho fundamental del habeas data, configurándolo como una garantía del derecho a la intimidad. Analiza también otros aspectos importantes para ese momento como el hecho de que no existían en ese momento herramientas eficaces para proteger el derecho a la intimidad y que es necesario hacer un uso responsable de la informática

GUIA DE ANALISIS JURISPRUDENCIAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 03 de 08/05/2016
Propósito del diligenciamiento: Obtener la información pertinente sobre la posición jurisprudencial de la Corte Constitucional acerca del análisis de constitucionalidad de la ley estatutaria de protección de datos personales. De esta manera se va a identificar el desarrollo de la línea jurisprudencial	
Identificación de la Providencia	
Corporación y Sala	Corte Constitucional colombiana
Sentencia N°	T-729
Medio de Acción	Control de constitucionalidad previo
Fecha	5 de septiembre de 2002
Magistrado Ponente	Eduardo Montealegre Lynett

1. Posición jurídica de la parte actora

a) Hechos Relevantes:

- El departamento administrativo de Catastro del Distrito de Bogotá dispuso la publicación en internet la base de datos sobre la información catastral de Bogotá. Sólo se requiere saber el número de identificación de la persona para conocer datos del inmueble que este a su nombre. También al digitar otros cuatro dígitos (dirección del predio, matrícula inmobiliaria, código homologado de información predial, cédula catastral y documento de identidad) puede conocerse información más personal y económica.
- La Superintendencia de Salud hace lo propio con la publicación de los datos del afiliado al régimen de seguridad social en salud, sus meses en mora y beneficiarios.
- El accionante considera vulnerado su derecho a la vida, integridad personal, propiedad, libertad.

b) Argumentos Jurídicos del Accionante

El accionante considera vulnerado su derecho a la intimidad, a la vida, integridad personal, propiedad, libertad.

c) Pretensiones.

Que se suspenda la publicación de la información.

2. Posición jurídica del demandado

e) Excepciones aducidas por la Entidad Demandada

No hubo

f) Argumentos jurídicos del Demandado

No hubo

3. Planteamiento del problema jurídico

¿La posibilidad de acceder a información sobre personas naturales, mediante la digitación del número de identificación, gracias a la manipulación de ciertas bases de datos dispuestas en la Internet, desconoce los derechos fundamentales de los ciudadanos referenciados en las mismas?

4. Fallo de Instancia

a) Consideraciones

“(…)primero, que con la publicación de información mediante las referidas páginas de Internet no se presenta intromisión irracional en la órbita reservada del actor, ni se divulgan hechos privados ni hechos tergiversados o falsos.

Segundo, que en cumplimiento del principio de eficiencia de la administración pública, las entidades del Estado están en la obligación de adoptar esta clase de mecanismos de información.

Tercero, que frente a la página de la Superintendencia de Salud, con la racionalización y publicación de la información, se pretende la calidad en la prestación del servicio de salud y el control de los recursos de los asociados, en cumplimiento de lo ordenado por el artículo 3 del decreto 1259 de 1994.

Y cuarto, que frente a la página de Catastro, la información dispensada tras la digitación del número de identificación es la general o básica del predio, la cual es de dominio público, y que por otro lado, para obtener información jurídica y económica, se requiere la digitación de datos adicionales que al ser de carácter privado, restringen la posibilidad de acceso a la misma.”

b) Decisión de Primera Instancia

Denegar la tutela impetrada pues no se pone en peligro al tutelante en su integridad ya que arroja información que corresponde a la generalidad de los usuarios con vías a cumplir los fines y propósitos de esta institución.

5. De la segunda instancia

NO APLICA

a) Consideraciones respecto al problema jurídico

b) Tesis de la Corporación

c) Fundamentos de la Tesis de la Corporación

d) Salvamentos de voto

6. Revisión de tutela

a) Consideraciones respecto al problema jurídico

Para estos efectos la Sala se pronunciará sobre (a) el contenido y alcance del derecho constitucional al habeas data o a la autodeterminación informática; (b) los principios de la administración de las bases de datos; (c) los datos personales y las diversas clasificaciones de la información; y (d) la deficiencia en los mecanismos de protección de derechos fundamentales relacionados con el manejo de las bases de datos y la necesidad de regulación.

(...)

El derecho fundamental al habeas data, es aquel que otorga la facultad al titular de datos personales, de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales.

(...)

En concepto de la Corte, se entiende por el proceso de administración de datos personales, las prácticas que las entidades públicas o privadas adelantan con el fin de conformar, organizar y depurar bases de datos personales, así como la divulgación de estos últimos en un contexto claramente delimitado y con sujeción a ciertos principios.

(...)

Para la Sala, la diferenciación y delimitación de los derechos consagrados en el artículo 15 de la Constitución, cobra especial importancia por tres razones: (i) por la posibilidad de obtener su protección judicial por vía de tutela de manera independiente; (ii) por la delimitación de los contextos materiales que comprenden sus ámbitos jurídicos de protección; y (iii) por las particularidades del

régimen jurídico aplicable y las diferentes reglas para resolver la eventual colisión con el derecho a la información.

Para la Sala, reiterando la Jurisprudencia de la Corte, el proceso de administración de los datos personales se encuentra informado por los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad.

(...)

Los datos personales, por sus condiciones especiales, prima facie se encuentran fuera de la órbita de conductas protegidas por el régimen general del derecho constitucional a la información. En consecuencia, la colisión entre derecho al habeas data o derecho a la autodeterminación informática y derecho a la información, deberá resolverse atendiendo las particularidades tanto de la información, convertida en datos personales, como de los rasgos y poder de irradiación del derecho a la autodeterminación informática

(...)

Ante la inexistencia de mecanismos ordinarios de protección de los derechos relacionados con la libertad informática, y la ausencia de una ley estatutaria que regule con amplitud esta materia, situación denunciada en múltiples oportunidades por esta Corte, y aceptando que la acción de tutela a pesar de su especial importancia en materia de protección de los derechos al habeas data y a la intimidad, no constituye herramienta suficiente para la reconducción adecuada de las conductas desarrolladas en el ámbito del poder informático(...) es necesario que el acceso a la información personal debidamente administrada se realice bajo dos principios, llamados a operar bajo la premisa de la posición de garante[36] de la entidad administradora y del peticionario: el principio de responsabilidad compartida, según el cual, tanto quien solicita la información como quien la suministra, desarrollen su conducta teniendo en cuenta la existencia de un interés protegido en cabeza del titular del dato. Y el principio de cargas mutuas, según el cual, a mayor información solicitada por un tercero, mayor detalle sobre su identidad y sobre la finalidad de la información.

b) Tesis de la Corporación

La Sala comparte la opinión del representante de Catastro, en el sentido de afirmar que la información disponible con la digitación del número de cédula es precaria, y que para el acceso a información específica sobre los diversos bienes inmuebles registrados, es necesario reunir cuatro de cinco datos posibles. Datos que, por el carácter confidencial de los mismos, hacen imposible que terceros totalmente ajenos al titular del número de identificación, tengan acceso a información pormenorizada de los diversos bienes.

(...)

Sin embargo, para la Corte, la recopilación y publicación de la información contenida en la base de datos de Catastro, está sometida a los principios de la administración de datos, precisamente por que la misma está conformada por datos personales mediante los cuales se asocia una realidad patrimonial con una persona determinada. La Sala, al examinar en el caso concreto el poder de irradiación de estos principios como manifestación del derecho a la autodeterminación informática, encuentra que se presenta una vulneración de los derechos fundamentales del señor Carlos Antonio Ruiz Gómez.

(...)

En conclusión, *a partir de la inobservancia y desconocimiento de los principios de libertad, finalidad*

e individualidad, rectores de la administración de datos personales, la Sala considera lo siguiente: con la publicación de la base de datos sobre la información catastral de Bogotá en la Internet, tal y como está dispuesta, el Departamento administrativo de Catastro Distrital de Bogotá, vulnera el derecho fundamental a la autodeterminación informática del señor Carlos Antonio Ruiz Gómez.

Sobre la información personal puesta por la superintendencia de salud

En este aspecto, la Sala considera que la información disponible tras la digitación del número de identificación, al estar referida a datos personales del actor que tienen la virtud de revelar aspectos de su órbita privada (su condición de afiliado o no, la condición de beneficiarios de ciertas personas, la EPS a la cual se encuentra afiliado, si está o no en mora, la fecha de afiliación, las posibles modificaciones en la afiliación, etc.), se encuentra sometida a los principios de la administración de datos personales, en los términos de esta sentencia.

(...)

Considera entonces la Corte que, con la publicación de la base de datos sobre los afiliados al sistema integral de seguridad social en Salud, la Superintendencia Nacional de Salud vulnera el derecho fundamental a la autodeterminación informática del señor Carlos Antonio Ruiz Gómez. En efecto, toda vez que este tipo de datos personales está catalogado como información semi-privada, es decir que su acceso se encuentra restringido, la posibilidad de su conocimiento por parte de terceros totalmente ajenos al ámbito propio en el cual se obtuvo dicha información, a partir del sencillo requisito de digitar su número de identificación, *desconoce los principios constitucionales de libertad, finalidad, circulación restringida e individualidad propios de la administración de datos personales*.

c) Fundamentos de la Tesis de la Corporación

Sobre la publicación de datos de catastro que viola el habeas data:

1.) En primer lugar, la conducta de Catastro *no se ajusta al principio de libertad*, vacilar en los procesos de administración de datos. Según este principio, la publicación y divulgación de la información, debe estar precedida de autorización expresa y libre de vicios del titular de los datos. Encuentra la Sala que, esta circunstancia no fue atendida por Catastro, quien procedió a la publicación de la base en la Internet, sin el consentimiento previo del señor Carlos Antonio Ruiz.

2.) En segundo lugar, la conducta de Catastro *desconoce de manera indirecta el principio de finalidad*, en cuanto que permite el acceso indiscriminado a la información personal del señor Carlos Antonio Ruiz a través de su publicación en la Internet. Para la Corte, el proceso de administración de datos personales debe obedecer a una finalidad definida de manera clara y previa, que en el caso de catastro se concreta en la posibilidad de acceso a la información predial en determinadas condiciones y por ciertas personas naturales o jurídicas. En este sentido, Catastro, al facilitar el acceso a información personal de manera indiscriminada, distorsiona la finalidad a la cual estaba llamada la base de datos, pues permite que extraños, sin intereses visibles, accedan a la información sin que sea posible ningún tipo de control por parte de sus titulares.

3.) En tercer lugar, las condiciones de acceso indiscriminado a la información, aunque esta sea precaria, constituyen un riesgo cierto que debe ser evitado ante la posible elaboración de perfiles virtuales. *Esta situación conduce a analizar el acance del principio de individualidad*. Según este principio, el Departamento Administrativo de Catastro, como administrador de datos personales, debe abstenerse de realizar conductas que faciliten el cruce de datos y la construcción de perfiles individuales. Nuevamente encuentra la Corte que, Catastro, con la publicación de información

patrimonial del señor Carlos Antonio Ruiz Gómez, al facilitar las condiciones para que la misma sea sumada a otra, con el concurso de diversas fuentes de información, vulnera su derecho a la autodeterminación informática.

Sobre la publicación de datos de salud de la persona:

Según *el principio de finalidad*, los datos, además de procurar un objetivo constitucionalmente protegido, deben conservar el propósito por el cual fueron suministrados u obtenidos, el cual está determinado generalmente por los ámbitos específicos en los que dicha operación se realiza y que en este caso es el propio de las relaciones privadas entre el titular de los datos y las entidades de la seguridad social.

Este principio, *ligado al de la circulación restringida*, indica que efectivamente la información personal del señor Carlos Antonio Ruiz Gómez, por ser información semi-privada, está llamada a circular exclusivamente dentro de las entidades que conforman el sistema integral de seguridad social en salud.

7. Análisis Crítico

a) Identificación de precedentes

Sobre los principios para la administración de datos personales: T-022 de 1993, T-097 de 1995, T-552 DE 1997, SU-028 DE 1995, Tt-176, T-307 de 1999, T-119 de 1995, T-414 de 1992.

b) Reglas aplicadas

c) Comentario

Se discrepa respecto a la afirmación de que la información pública puede ser obtenida sin reserva alguna sin importar si es privada o personal. Pues la naturaleza de la información no deja de ser personal por el hecho de que sea de conocimiento público y por tanto requiere el consentimiento del titular.

GUIA DE ANALISIS JURISPRUDENCIAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 04 de 08/05/2016
Propósito del diligenciamiento: Obtener la información pertinente sobre la posición jurisprudencial de la Corte Constitucional acerca del análisis de constitucionalidad concreta en el derecho fundamental protección de datos personales.	
Identificación de la Providencia	
Corporación y Sala	Corte Constitucional colombiana
Sentencia N°	SU-082
Medio de Acción	Acción de tutela
Fecha	1 de marzo de 1995
Magistrado Ponente	Jorge Arango Mejía

1. Posición jurídica de la parte actora

a) Hechos Relevantes:

- El actor solicitó un crédito a Servicios financieros S.A., por dificultades económicas se puso en mora y fue reportado por esta sociedad como deudor moroso a DATA CREDITO de Computec S.A.
- El demandante pagó su deuda, le entregaron paz y salvo el 25 de Junio de 1993. Sin embargo su nombre aparece reportado en datacredito. Por lo anterior el actor no ha podido acceder a crédito ni ser garante de obligaciones
- Acudió a la Regional Medellín de la Defensoría del Pueblo para que le protegieran y ayudaran.

b) Argumentos Jurídicos del Accionante

c) Pretensiones.

El actor solicita que se le tutele el derecho fundamental a la intimidad consagrado en el artículo 15 de la Constitución.

2. Posición jurídica del demandado

- g) Excepciones aducidas por la Entidad Demandada
- h) Argumentos jurídicos del Demandado

3. Planteamiento del problema jurídico

En el caso que nos ocupa, la pregunta que debe contestarse es ésta: ¿existe un derecho de los establecimientos de crédito a recibir información veraz sobre la conducta de sus posibles deudores en lo tocante al cumplimiento de sus obligaciones? Y, de otra parte, ¿tiene el deudor derecho a impedir que el acreedor informe sobre la manera como él cumplió o cumple sus obligaciones?

4. Fallo de Instancia

a) Consideraciones

“(…) si bien la Corte Constitucional en casos como el presente ha tutelado los derechos aquí invocados, en el presente caso "es necesario analizar el contenido del registro, su objetividad, si es completo, las condiciones legales de su manejo o circulación, el consentimiento expreso del titular y el término para la utilización razonable de los datos, para determinar los efectos que el uso de la información puede tener sobre la vida y las posibilidades presentes y futuras de la persona.”

b) Decisión de Primera Instancia

Negar el amparo solicitado.

5. De la Segunda Instancia NA

- e) Consideraciones respecto al problema jurídico
- f) Tesis de la Corporación
- g) Fundamentos de la Tesis de la Corporación
- h) Salvamentos de voto

6. Revisión de tutela NA

a) Consideraciones respecto al problema jurídico

Cuando el artículo 15 de la Constitución consagra el derecho a la intimidad personal y familiar, es evidente que ampara, en primer lugar, aquello que atañe solamente al individuo, como su salud, sus hábitos o inclinaciones sexuales, su origen familiar o racial, sus convicciones políticas y religiosas. Ampara, además, la esfera familiar, lo que acontece en el seno de la familia, que no rebasa el ámbito

doméstico. Nadie extraño tiene, en principio, por qué conocer cómo discurre la vida familiar. Sólo en circunstancias anormales, y precisamente para volver a la normalidad, el Estado, por ejemplo, interviene, y temporalmente el derecho a la intimidad familiar debe ceder frente a otro superior.

“(…) quien obtiene un crédito de una entidad dedicada a esta actividad y abierta al público, no puede pretender que todo lo relacionado exclusivamente con el crédito, y en especial la forma como él cumpla sus obligaciones, quede amparado por el secreto como si se tratara de algo perteneciente a su intimidad. Lo anterior sin perjuicio de lo que se señalará sobre la titularidad del dato personal, en otra parte de esta sentencia.”

El artículo 15 de la Constitución garantiza también el derecho al buen nombre. (...)El derecho al buen nombre no es una abstracción, algo que pueda atribuírse indiscriminadamente a todas las personas. En los casos concretos habrá que ver sin quien alega que se le ha vulnerado, lo tiene realmente.

En lo que tiene que ver con el manejo del crédito, es evidente que la fama de buen o mal pagador se origina en la forma en que usualmente la persona atiende sus obligaciones. Es ella misma quien realiza los actos que configuran su fama.

Es elemental, por lo dicho, que la vulneración del buen nombre sólo puede aducirla quien lo tiene, porque lo ha ganado.

De otra parte, es claro que el buen nombre es un concepto diferente por completo a la intimidad personal y familiar: ésta es secreta para los demás, en tanto que aquél es público por naturaleza, y lo que es público por naturaleza no puede tornarse en íntimo, porque sería inadecuado.

El artículo 20 de la Constitución consagra el derecho a informar y a recibir información veraz e imparcial. ¿Qué es una información veraz? Sencillamente, la que corresponde a la verdad. Pero no a una verdad a medias, sino a la verdad completa.

¿Cuál es el núcleo esencial del **habeas data**? A juicio de la Corte, está integrado por el **derecho a la autodeterminación informática** y por la **libertad**, en general, y en especial económica.

El sujeto activo del derecho a la autodeterminación informática es toda persona, física o jurídica, cuyos datos personales sean susceptibles de tratamiento automatizado.

El sujeto pasivo es toda persona física o jurídica que utilice sistemas informáticos para la conservación, uso y circulación de datos personales. En la materia de que trata esta sentencia, tales datos deberán referirse a la capacidad económica de la persona, y, concretamente, a la manera como ella atiende sus obligaciones económicas para con las instituciones de crédito.

El contenido del habeas data se manifiesta por tres facultades concretas que el citado artículo 15 reconoce a la persona a la cual se refieren los datos recogidos o almacenados:

- a) El derecho a conocer las informaciones que a ella se refieren;
- b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos;
- c) El derecho a rectificar las informaciones que no correspondan a la verdad.

Existe, además, el derecho a la caducidad del dato negativo, no consagrado expresamente en el artículo 15 de la Constitución, pero que se deduce de la misma autodeterminación informática, y también de la libertad. El alcance de este derecho se analizará posteriormente, en esta misma providencia.

Hay que aclarar que la actualización, y la rectificación de los datos contrarios a la verdad, son, en principio, obligaciones de quien maneja el banco de datos; y que si él no las cumple, la persona concernida puede exigir su cumplimiento.

Además, para facilitar el conocimiento de los datos por la persona concernida, debe notificarse a ésta sobre la inclusión de tales datos en el banco. La oportunidad para tal notificación, también debe ser definida por el legislador.

(...)

Obsérvese que cuando un establecimiento de crédito solicita información sobre un posible deudor, no lo hace por capricho, no ejerce innecesariamente su derecho a recibir información. No, la causa de la solicitud es la defensa de los intereses de la institución que, en últimas, son los de una gran cantidad de personas que le han confiado sus dineros en virtud de diversos contratos.

El deudor, por su parte, no tiene derecho, en el caso que se examina, a impedir el suministro de la información, principalmente por tres razones. La primera, que se trata de hechos que no tienen que ver solamente con él; la segunda, que no puede oponerse a que la entidad de crédito ejerza un derecho; y la tercera, que no se relaciona con asuntos relativos a su intimidad. Lo anterior, bajo el entendido que la circulación de esa información está condicionada a la autorización previa del interesado, como se explicará más adelante

(...)

Se ha dicho que **la información para ser veraz debe ser completa**. En lo atinente a un crédito, por ejemplo, un banco no daría información completa, si se limitara a expresar que el deudor **ya no debe nada y ocultara el hecho de que el pago se obtuvo merced a un proceso de ejecución, o que la obligación permaneció en mora por mucho tiempo. Igualmente, no sería completa si no se informara desde qué fecha el cliente está a paz y salvo.**

Y el derecho que quien fue deudor moroso tiene a que se ponga al día la información, exige que se registre no sólo el pago, voluntario o forzado, sino la fecha del mismo, como hechos nuevos. No que se borre todo lo anterior, como si no hubiera existido. Sostener lo contrario llevaría al absurdo de afirmar que actualizar una historia, es consignar únicamente el último episodio, eliminando todo lo anterior.

(...)

En conclusión: mientras la información sobre un deudor sea veraz, es decir, verdadera y completa, no se puede afirmar que el suministrarla a quienes tienen un interés legítimo en conocerla, vulnera el buen nombre del deudor. Si realmente éste tiene ese buen nombre, la información no hará sino reafirmarlo; y si no lo tiene, no podrá alegar que se le vulnera.

Como se ha visto, el deudor tiene derecho a que la información se actualice, a que ella contenga los hechos nuevos que le beneficien.

Y, por lo mismo, también hacia el pasado debe fijarse un límite razonable, pues no sería lógico ni justo que el buen comportamiento de los últimos años no borrara, por así decirlo, la mala conducta pasada.

¿Qué ocurre en este caso? Que el deudor, después de pagar sus deudas, con su buen comportamiento por un lapso determinado y razonable ha creado un buen nombre, una buena fama, que en tiempos pasados no tuvo.

Corresponde al legislador, al reglamentar el habeas data, determinar el límite temporal y las demás condiciones de las informaciones. Igualmente corresponderá a esta Corporación, al ejercer el control de constitucionalidad sobre la ley que reglamente este derecho, establecer si el término que se fije es razonable y si las condiciones en que se puede suministrar la información se ajustan a la Constitución.

Pero, mientras no lo haya fijado, hay que considerar que es razonable el término que evite el abuso del poder informático y preserve las sanas prácticas crediticias, defendiendo así el interés general.”

b) Tesis de la Corporación

Existiendo la autorización necesaria por parte del actor, para que los datos relativos a su comportamiento comercial sean suministrados y consultados, esta Sala de Revisión no encuentra vulneración alguna de sus derechos fundamentales. Así mismo, la información que se está suministrando está actualizada, pues en ella se especifica que el actor ya canceló su crédito. Sin embargo, no es completa, pues no se está incluyendo la fecha en que el actor empezó a estar en mora, como tampoco en que momento dejó de estarlo. Dato éste de gran importancia, pues a partir de él se puede establecer con certeza cuál ha sido la línea de comportamiento comercial del actor.

c) Fundamentos de la Tesis de la Corporación

Lo expuesto en esta providencia, en relación con el derecho a la información y la legitimidad de la conducta de las entidades que solicitan información de sus eventuales clientes, a las centrales de información que para el efecto se han creado, así como la facultad de reportar a quienes incumplan las obligaciones con ellos contraídas, tiene como base fundamental y punto de equilibrio, la autorización que el interesado les otorgue para disponer de esa información, pues al fin y al cabo, los datos que se van a suministrar conciernen a él, y por tanto, le asiste el derecho, no sólo a autorizar su circulación, sino a rectificarlos o actualizarlos, cuando a ello hubiere lugar.

Autorización que debe ser expresa y voluntaria por parte del interesado, para que sea realmente eficaz, pues de lo contrario no podría hablarse de que el titular de la información hizo uso efectivo de su derecho. Esto significa que las cláusulas que en este sentido están siendo usadas por las distintas entidades, deben tener una forma y un contenido que le permitan al interesado saber cuáles son las consecuencias de su aceptación.

(...)

Con el fin de establecer si en el presente caso, se cumplieron las condiciones antes descritas, para que el nombre del señor Gabriel Alberto González Mazo, aparezca reportado ante las distintas centrales de información, la Sala solicitó a las distintas entidades que aparecen relacionadas por Datacrédito, informar si el aquí demandante, "... al momento de suscribir los respectivos contratos de cuenta corriente o tarjeta de crédito autorizó expresamente, la inclusión de informaciones relacionadas con su comportamiento comercial, hábitos de pago, manejo de su cuenta, etc., manejados por alguna entidad autorizada para el efecto, lo mismo que el suministro de tales informaciones a quienes tuvieren interés legítimo en ellas...".

Como respuesta a esta petición, Invercrédito servicios financieros S.A. informó que el actor al

momento de solicitar el crédito y suscribir el pagaré correspondiente, aceptó una cláusula que dice " Autorizo a Invercrédito S.A.... para fines estadísticos y de información sobre riesgos crediticios a suministrar y/o solicitar a otras entidades de crédito información sobre saldos a mi cargo". Igualmente señaló que, el actor presentó mora en el pago de su obligación hasta por cuatro (4) meses, crédito que en la actualidad está totalmente cancelado.

Por su parte, el Banco Popular informó que el actor al momento de suscribir el contrato de cuenta corriente consintió en una cláusula del mismo, que le permite a la entidad suministrar a las centrales de información o de riesgo, los datos relacionados con las operaciones de crédito que el actor celebre o llegue a celebrar con ellos.

7. Análisis Crítico

- a) Identificación de precedentes
- b) Reglas aplicadas
- c) Comentario

La formulación del contenido esencial del derecho al habeas data, de la reafirmación del derecho al buen nombre y su conexidad con el primero. La definición de los elementos estructurales del derecho al habeas data identificando sujeto activo, sujeto pasivo y las obligaciones de este último. Todos estos valiosos elementos iniciales para la formulación del contenido del derecho al habeas data.

GUIA DE ANALISIS JURISPRUDENCIAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 05 de 08/05/2016
Propósito del diligenciamiento: Obtener la información pertinente sobre la posición jurisprudencial de la Corte Constitucional acerca del análisis de constitucionalidad concreta en el derecho fundamental protección de datos personales.	
Identificación de la Providencia	
Corporación y Sala Sentencia N° Medio de Acción Fecha Magistrado Ponente	Corte Constitucional colombiana T-814 Acción de tutela 17 de septiembre de 2003 Rodrigo Escobar Gil

1. Posición jurídica de la parte actora

- a) Hechos Relevantes:
 - La demandante es suscriptora del servicio de telefonía prestado por las empresas demandadas.
 - Durante dos meses, no canceló el servicio de telefonía prestado por dichas entidades, por lo cual éstas suspendieron el servicio.
 - Además de la suspensión del servicio, las entidades demandadas instalaron un mecanismo mediante el cual, cada vez que alguien marca su número de teléfono suena una grabación en la que se informa a quien llama, que el número marcado fue desconectado por falta de pago.
- b) Argumentos Jurídicos del Accionante

- La demandante considera que las dos entidades demandadas están publicitando la deuda que tiene con ellas. Sostiene que esta publicidad por vía telefónica, le configura un perjuicio moral y material, toda vez que las personas que marcan su número, se enteran de su situación financiera. Por lo tanto, esta conducta altera su tranquilidad y sus derechos al buen nombre y al trato igualitario frente a los demás usuarios del sistema.
- Sostiene además, que esta conducta es propia de la delincuencia, y que no está permitida por la Constitución ni por la ley, ya que “los chepitos fueron proscritos por la propia Corte”.

c) Pretensiones.

La demandante solicita que se protejan sus derechos al buen nombre y a la igualdad, presuntamente vulnerados por las entidades demandadas, y que no se siga difundiendo la deuda que tiene con dichas empresas cada vez que alguien marca el número de teléfono de su residencia.

2. Posición jurídica del demandado

- a) Excepciones aducidas por la Entidad Demandada NO PROPUSIERON
 b) Argumentos jurídicos del Demandado

Respuesta del representante de Telbuenaventura

El representante legal de Telebuenaventura S.A. E.S.P., afirma que esta empresa efectivamente es el operador del servicio telefónico en esa ciudad. En esa medida, suscribió un contrato de condiciones uniformes con la demandante, en el cual se establece la suspensión como consecuencia de la falta de pago de dos facturas consecutivas. Sostiene que la demandante adeuda cuatro facturas, razón por la cual le fue suspendido el servicio.

Informa que la empresa demandada ha enviado varios oficios a Telecom, quien opera la central telefónica en el centro de la ciudad, para que la “música” que anuncia la deuda de la demandante sea retirada. A pesar de ello, indica que estas comunicaciones no han tenido efecto en este caso. Por otra parte, sostiene que esta música hace referencia a Telecom, y no a Telebuenaventura, con lo cual aduce que fue aquella, y no ésta la que instaló el mecanismo de grabación.

Respuesta del representante de Telecom

Además de reiterar la información en relación con la mora de la demandante, el representante de Telecom sostiene que la grabación que instala la empresa en nada vulnera los derechos de los deudores. Afirma que se trata de dos grabaciones distintas. Una de ellas, la que escuchan quienes marcan el número asignado al deudor, informa que la línea se encuentra suspendida, sin especificar la razón, que puede ser distinta a la falta de pago. La otra, que escucha únicamente el deudor, o quien descuelga el auricular en su residencia, es de carácter personal, y lo invita a arreglar su situación financiera con la empresa.

3. Planteamiento del problema jurídico

¿La instalación de los mensajes por parte de Telecom, constituye un mecanismo sancionatorio que amenaza o vulnera los derechos fundamentales de la demandante?

4. Fallo de Instancia

a) Consideraciones

En particular, sostiene que en ningún momento se vulneraron los derechos a la intimidad o al buen nombre, porque la grabación que escuchan las personas que llaman a la línea no precisa la razón por la cual se encuentra suspendida. En esa medida, no es cierto que se esté difundiendo información acerca de la deuda de la demandante. Por otra parte, la grabación que invita al usuario a ponerse al día en la cuenta tampoco publicita la deuda, toda vez que ésta la escucha únicamente escucha el usuario al levantar el auricular del teléfono cuya línea se encuentra suspendida.

b) Decisión de Primera Instancia

El juzgado tercero penal de Circuito de Buenaventura niega el amparo solicitado. “Para adoptar su decisión, el juzgado de primera instancia toma como punto de partida el contenido de la comunicación que se escucha al marcar el número suspendido, el cual considera que no vulnera el derecho a la intimidad o al buen nombre del demandante.”

5. De la Segunda Instancia

a) Consideraciones respecto al problema jurídico

“En concepto del tribunal de segunda instancia, el mensaje que informa que el número telefónico se encuentra suspendido tiene una finalidad persuasiva, que pretende que el usuario se vea sometido a la presión producida por el conocimiento público de su condición de deudor del servicio de telefonía. Sin embargo, agrega, este mecanismo resulta innecesario, pues la ley 142 de 1994, establece los medios necesarios para que las empresas prestadoras de servicios públicos recuperen las deudas de los usuarios. Siendo titulares de prerrogativas que privilegian su posición contractual, como lo son la suspensión y cancelación del servicio, y el cobro ejecutivo de las facturas adeudadas, las empresas de servicios públicos no pueden hacer uso de mecanismos adicionales no previstos en la ley, para obtener el pago del servicio.”

b) Tesis de la Corporación

“El Tribunal Superior de Distrito Judicial de Buga –Sala Penal-, mediante Sentencia de febrero 28 de 2003 decidió revocar la Sentencia de primera instancia, y en su lugar conceder la protección solicitada, ordenando a las empresas accionadas desinstalar la grabación que informa a quienes llaman, que la línea telefónica ha sido suspendida. Así mismo, advierte a dichas entidades que en el futuro se abstengan de realizar conductas que atenten contra los derechos de la demandante.”

6. Revisión de la Corte Constitucional

a) Consideraciones respecto al problema jurídico

“El derecho al buen nombre ha sido definido por esta Corporación, como la protección que se

otorga a los individuos frente a la difusión de informaciones que no correspondan a la realidad, y que en esa medida, alteren injustificadamente la reputación que tienen en su entorno social.”

“- El derecho al buen nombre es esencialmente un derecho de valor porque se construye por el merecimiento de la aceptación social, esto es, gira alrededor de la conducta que observe la persona en su desempeño dentro de la sociedad. La persona es juzgada por la sociedad que la rodea, la cual evalúa su comportamiento y sus actuaciones de acuerdo con unos patrones de admisión de conductas en el medio social y al calificar aquellos reconoce su proceder honesto y correcto. Por lo tanto, **no es posible reclamar la protección al buen nombre cuando el comportamiento de la persona no le permite a los asociados considerarla como digna o acreedora de un buen concepto o estimación.**” (Resaltado fuera de texto) SU-056 de 1995, M.P. Antonio Barrera Carbonell.

El derecho al buen nombre que garantiza el deber de veracidad, siempre que la información que transmitan sea “(...) veraz, completa y precisa, que para ese caso significa que esté actualizada (...)” “(...) en relación con los diferentes posibles emisores de información”. Adicionalmente señala el principio de imparcialidad que puede comprobarse a partir de la de los indicios que da la buena fe del emisor y la necesidad de que la información sea difundida, pues la intimidad y la privacidad de ella en principio impiden la libertad de información o libertad de expresión por las consecuencias sociales potencialmente nefastas que traería la difusión de aspectos íntimos o sensibles de la persona. Hay que tener presente las consecuencias de la difusión, su frecuencia e intensidad y el canal utilizado.

“La importancia que socialmente se le otorga a algunos de tales aspectos, implica un mayor compromiso del buen nombre y de la honra de las personas, y por lo tanto, un mayor rigor en el manejo de la información. A manera de ejemplo, puede afirmarse que al transmitir información respecto de la responsabilidad penal de una persona, el emisor debe tener mayor cuidado que cuando se refiere a otros aspectos de la persona. De tal manera, la responsabilidad por la transmisión de la información será mayor o menor, dependiendo de su naturaleza.”

“Por lo tanto, no se accederá a la protección solicitada en relación con el derecho al buen nombre de la demandante.”

“La realización de los principios de eficiencia y universalidad en la prestación de los servicios públicos domiciliarios requiere que los usuarios cancelen oportunamente sus deudas con las empresas que los prestan (...) En esta medida, es completamente razonable que las empresas hagan uso de todos los mecanismos legales a su alcance para recaudar el pago por los servicios públicos domiciliarios que ellas prestan. Sin embargo, aun cuando el recaudo de los servicios sea un objetivo razonable, no justifica la utilización de mecanismos desproporcionados que afecten los derechos fundamentales de los usuarios.”

Frente a las intromisiones del Estado y la sociedad en diversos aspectos de la vida de los individuos surge la protección de la privacidad a través de dos derechos: derecho a la privacidad en sentido general donde se puede negar la intromisión de terceros en las actuaciones privadas que le concierne, si se quiere, y derecho a la autodeterminación

informativa, para evitar que la información personal se divulgue. “Por tal motivo, al sopesar la intimidad frente a otros derechos y libertades, es necesario tener en cuenta el grado de invasión de la esfera privada.”

b) Tesis de la Corporación

La Corte Constitucional considera adecuado analizar el efecto de las dos grabaciones sobre los derechos fundamentales de la demandante.

La primera grabación, la que afirma que está sin servicio por estar en mora, no afecta el derecho fundamental porque las personas pueden comunicarse por otros medios distintos al telefónico y que adicionalmente no se dice nada fuera de la verdad: que se encuentra suspendido el servicio sin mermar su credibilidad económica.

La segunda grabación, la que invita a pagar a los miembros de la casa donde esta alojada la línea telefónica viola el derecho a la intimidad y la privacidad porque es un mecanismo de presión psicológica que afirma al ser humano como un medio para lograr que pague la factura que tiene en mora.

c) Fundamentos de la Tesis de la Corporación

“En el presente caso, puede sostenerse que la grabación que invita a cancelar la deuda no constituye una intromisión en el ámbito interno del hogar de la demandante, pues ésta sólo se escucha cuando alguien descuelga el teléfono. (...)¿Cuál es el objeto de instalar una grabación que sólo escuchan los habitantes de una residencia, en la que se les invita a cancelar una deuda que ya conocen? Precisamente por tratarse de una línea suspendida, la grabación carece de objeto si no es como mecanismo de presión a los usuarios morosos. En esa medida, el objeto de la grabación trasciende lo meramente informativo.” Este mecanismo de presión supone ignorar el principio de libertad y responsabilidad del ser humano en su dignidad, pues afirma que a partir de la presión es que se motiva a lograr hacer las cosas

6. Análisis Crítico

NO APLICA

- d) Identificación de precedentes
- e) Reglas aplicadas
- f) Comentario
- g)

GUIA DE ANALISIS JURISPRUDENCIAL	
OBSERVADOR : Camilo José Puello Rincón	GUIA N° 06 de 22/05/2016
Propósito del diligenciamiento: Obtener la información pertinente sobre la posición jurisprudencial del Tribunal Constitucional Federal de Alemania acerca de la ley del censo de 1983 que permitió formular el derecho a la autodeterminación informativa vinculado al derecho a la personalidad y a dignidad humana	

Identificación de la Providencia	
Corporación y Sala	Tribunal Constitucional de Alemania
Sentencia N°	1 BvR 209/83
Medio de Acción	Recurso de inconstitucionalidad alemana
Fecha	15 de diciembre de 1983
Magistrado Ponente	NA

1. Posición jurídica de la parte actora

- a) Hechos Relevantes: NO APLICA
- b) Argumentos Jurídicos del Accionante: Se demanda por inconstitucional la ley sobre censo de población, profesiones, viviendas y centros de trabajo debido a que no se tiene claridad acerca del uso de los datos recolectados mediante la encuesta, existe el miedo de que puedan ser utilizados ilimitadamente porque la tecnología actual de tratamiento automatizado de datos ha evolucionado ostensiblemente. Por esas razones se considera que se encuentra ante una inminente afectación a la Ley Fundamental de Bonn. Sobre todo en los preceptos de recogida y utilización de datos personales.

Se viola el derecho a la propia personalidad debido a que no existe una obligación de volver anónimos los datos, por lo cual, así permanezcan almacenados en las bases de datos, existe el riesgo de que puedan repersonalizarse con el uso de la técnica, ya que permanecen en el censo fácilmente determinables. La información puede relacionarse con datos almacenados previamente y producir “una imagen total y pormenorizada de la persona respectiva – un perfil de la personalidad - , incluso del ámbito de su intimidad, convirtiéndose así el ciudadano en *hombre de cristal*” (P.136) Tampoco se informan frecuentemente del uso de sus datos personales al ciudadano para que pueda acusar la comisión del tipo penal de violación de secreto estadístico.

La transmisión nominativa de datos a los Ayuntamientos puede generar usos diferentes a los autorizados en las posibilidades estadísticas del tratamiento de datos pues hay una ambigüedad en las personas que puedan acceder a ellas y hacer uso de los datos. Esto por cuanto el interrogado sólo es informado de los fines de la encuesta, no de aquellos posteriores que surjan con la información.

- c) Pretensiones: Que se declaren inconstitucionales los artículos de la Ley del Censo de Población de 1983 aprobada por el *Bundestag* o Parlamento Federal de Alemania por violar los artículos 1,2,5 y 19 de la Ley Fundamental de Bonn que corresponden a los siguientes derechos:
- Derecho al libre desenvolvimiento de la personalidad y la dignidad humana.
 - Libertad de expresión
 - Garantías procesales

2. Posición jurídica del demandado

- a) Excepciones aducidas por la Entidad Demandada NO APLICA
- b) Argumentos jurídicos del Demandado

Los Gobiernos Federal y regionales de Baden-Württemberg, Baviera, Hamburgo, Baja Sajonia, Renania del Norte-Westfalia, Renania-Palatinado y Schleswig-Holstein afirman que es injustificado el recurso de inconstitucionalidad bajo el argumento de que las obligaciones quedan delimitadas al fin estadístico y a fines conexos que resultan de este último. La información ayudará a cumplir los deberes de la administración.

Los comisionados de protección de datos personales afirman que se cumplen las obligaciones al permitir controles de los órganos federales de protección de datos personales y del Ministerio Federal del Interior. La encuesta estadística es un medio para asegurar la anonimidad de manera suficiente.

Tampoco hay invasión a la privacidad debido a que se recolectan datos que no pertenecen a una esfera tan íntima, a que esos mismos datos al procesarse no permiten estructurar un perfil de la personalidad del individuo y a que permanecen inconexos de otras bases de datos.

El censo de población es el instrumento proporcional al logro de los fines, sin costos excesivos a largo plazo por la inexactitud de la información, menciona el caso de las bases de datos de enfermos, de catastro, de administración laboral o el caso de normas específicas que limitan su uso como los datos de renta por el secreto tributario.

El método de llevar personalmente los formularios por parte de contadores y luego ser remitidos por las personas en manera alguna afecta la intimidad.

El senado de Hamburgo por otro lado se opone diciendo que no hay garantías de que quede anónima la información, para ellos quedan dudas al respecto; es un presupuesto necesario para que el ciudadano facilite sus datos.

3. Planteamiento del problema jurídico

¿Violan los artículos de la Ley del Censo de 1983 los derechos establecidos en los artículos 1, 2,5 y 19 de la ley Fundamental de Bonn?

4. Fallo de Instancia

- a) Consideraciones NA
- b) Decisión de Primera Instancia NA

5. De la Segunda Instancia

- a) Consideraciones respecto al problema jurídico

El proyecto de ley fue una insistencia nueva acerca de la necesidad de hacer un censo sobre la población, las profesiones y los centros de trabajo según la distribución espacial y la composición, para así tomar decisiones en cumplimiento de la función estatal y también para necesidad de otras asociaciones y agremiaciones. El eje central es conocer la evolución y fundamento de los cambios que ocurrieron en Alemania para no incurrir en errores de planeación y decisiones malas.

Sobre las normas demandadas, se excluye el artículo 8 al no ser ocupantes o directores de establecimientos. También la norma del artículo 4 se excluye debido a que no son directores o propietarios de centros de trabajo o empresas. Hay pues una legitimidad por activa en lo demás dado que la ley de Alemania pide que sólo el directamente afectado puede interponer recursos de inconstitucionalidad.

Las demandas entonces son parcialmente fundadas.

b) Tesis de la Corporación

Sobre al artículo 5 no hay vulneración alguna pues la información de pertenencia a una asociación religiosa está amparada dentro de las excepciones de la ley fundamental al solicitarse mediante encuesta estadística.

En general ninguno de los preceptos de la ley del Censo viola el derecho fundamental del domicilio porque no aplica a la información que se consigue sin introducirse en la vivienda. Tampoco aplica la libertad de opinión negativa para evitar dar los datos, pues estos no son opiniones o pensamientos sino datos fácticos del interesado que proporciona.

Es incompatible el artículo 9°, párrafos 1 a 3 de la Ley del Censo de 1983, en cuanto que viola el derecho a la autodeterminación, de decidir para sí mismo las circunstancias en que revela situaciones de su propia vida. (P.153) “No serían compatibles con el derecho a la autodeterminación informativa un orden social y un orden jurídico que hiciese posible al primero, en el que el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo sabe algo de él.”(P.153) Este derecho cede ante los intereses sociales en que se desenvuelve, dentro de la comunidad de la que hace parte, por ejemplo para labores de planificación (P.157).

b) Fundamentos de la Tesis de la Corporación

“A consecuencia de lo que antecede, el grado de sensibilidad de las informaciones ya no depende únicamente de si afectan o no a procesos de la intimidad. Hace falta más bien conocer la relación de utilización de un dato para poder determinar sus implicaciones para el derecho de la personalidad.”(p.154)

“Sólo cuando reine la claridad sobre la finalidad con la cual se reclamen los datos y qué posibilidades de interconexión y de utilización existen se podrá contestar la interrogante sobre la licitud de las restricciones del derecho a la autodeterminación informativa” (P.154) Es por

esta razón que cuando se obligue a entregar información personal el legislador debe fijar el ámbito y el tipo de dato entregado, así como la finalidad, pues son decisiones que limitan el ejercicio del derecho. “Si, por el contrario, se trasladan para fines de pura administración ejecutiva(desviación de la finalidad) unos datos de referencia personal no anonimizados que se hayan recogido para objetivos estadísticos y estén destinados a ello según el ordenamiento legal, se cometería una intromisión ilícita en el derecho a la autodeterminación informativa”.(P.163)

La estadística tiene varios fines, no tiene uno sólo determinado, con la información puede relacionarse, puede fundamentarse decisiones. Esto no impide que sea limitada su actividad, esto se consigue al establecer requisitos especiales para para la recolección y elaboración de los datos. El secreto de los datos estadísticos es imprescindible para garantizar el derecho así como la anonimización pronta. “Si en consecuencia, sólo mediante la incomunicabilidad de las estadísticas cabe salvaguardar la actividad estatal de “planificación”, el principio del secreto y de la anonimización más pronta posible de los datos resulta obligado no sólo para la protección del derecho del individuo a la autodeterminación, sino también inherente a las estadísticas mismas” (P.157)

Los encargados independientes de la protección de datos son una salvaguarda del derecho a la autodeterminación informativa debido a las condiciones actuales de tratamiento de la información.

El legislador debe regular aspectos del deber de aclaración e ilustración, de la destrucción de datos que permitan identificar una persona, adoptar medidas para guardar la confidencialidad de la información y un contenido del formulario del censo ajustado a la ley.

c) Salvamentos de voto

NA

6. Análisis Crítico

a) Identificación de precedentes

b) Reglas aplicadas

- I. La protección de los datos personales del individuo ante su tratamiento y difusión indiscriminada debe hacerse en el marco del derecho general de protección de la persona que establece el artículo 2º, párrafo 1(1) en relación con el artículo 1º, párrafo 1(2) de la Ley Fundamental de Alemania. Este derecho se denomina autodeterminación informativa, su contenido da “(...) la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y la utilización de los datos referentes a su persona”.
- II. Las limitaciones serán establecidas cuando prioricen un interés superior que se fundamenta en la Constitución, en especial en lo referente al Estado Social de Derecho.
- III. Para imponer limitaciones debe acudir el legislador a los principios de proporcionalidad, claridad normativa y finalidad.
- IV. El principio de finalidad es imprescindible para apoyar la identificación de una vulneración del derecho a la autodeterminación informativa.

c) Comentario

Esta sentencia permitió analizar el surgimiento del proto-derecho al debido tratamiento de datos personales en el derecho a la autodeterminación informativa, que otorga la facultad a las personas en Alemania para conocer cómo se estaban almacenando y recolectando sus datos personales.

FIRMA

HERRAMIENTAS JURÍDICAS PARA LA PROTECCIÓN DE LOS DATOS
 PERSONALES EN COLOMBIA: ANÁLISIS DEL GRADO DE PROTECCIÓN JURÍDICA
 DEL HABEAS DATA

Herramientas jurídicas para la protección de datos personales en Colombia

*“La libertad desinhibida puede destruirse a sí misma.
 La voluntad liberada debe ser contenida a través de restricciones y sanciones,
 Que son los únicos límites que entiende (...)
 La soberanía de la voluntad desencadenada encuentra su complemento
 Y compañía perfecta en la soberanía del Estado”*
 Costas Douzinas,
El fin de los Derechos Humanos

Origen del derecho al Habeas Data en el Principio General de la Libertad³

Sobre el principio general de la libertad se hace la siguiente formulación: la posibilidad de hacer las cosas sin impedimento y por iniciativa propia. En esta pequeña frase se intenta condensar de manera inicial las definiciones encontradas en los estudios de filósofos del derecho y de la política sobre aquello que ha sido identificado como “libertad”, es decir, hacer lo más deseable y alcanzable. Hay un punto de partida común de todos ellos concentrado en el individuo quien se concibe autónomo, racional y en un contexto natural presupuesto que no tendrá impedimentos.⁴

Desde que han ocurrido las revoluciones políticas se ha pensado que el ser humano tiene como fin potenciar cada una de sus capacidades e iniciativas, lograr ser lo que el mismo desea, para lograrlo se ha asociado a la capacidad de no tener impedimentos per se, aquella de no recibir constricciones externas o ser influenciado para actuar contra lo que se desee que sea él

³Ver en este sentido Pérez Luño, A. (2005). Derechos Humanos, estado de derecho y Constitución. Madrid: Tecnos; Bobbio, N. (1998). Igualdad y libertad. Barcelona: Paidós.

⁴Tanto Jonh Locke como Thomas Hobbes construyen sus modelos contractualistas de Estado a partir de un hombre que era libre, natural y racional. Estas tres características unidas permitirán la asociación de personas en comunidad con distintas consecuencias según el tipo de corriente que defienda cada autor: liberalismo, con un individuo que debe permanecer aislado o sin molestias para ejercer la libertad de sus deseos o comunitarismo, donde la sociedad es esencial para que el individuo logre su libertad y su voluntad. Ver más en Nino, C (1988). El Liberalismo vs. Comunitarismo. En: *Revista de Estudios Constitucionales*. Madrid: CEPC. P.364 y ss.

mismo hombre, en su interioridad. Para lograrlo debe promoverse la mayor libertad posible, sin que dañe a otras personas, permitir que se desarrolle la naturaleza humana esencial en cada uno de nosotros y al mismo tiempo se logren satisfacer la iniciativa propia lo más eficientemente posible.

Frente a esto los estudiosos han identificado que la libertad humana tiene dos facetas interesantes: negativa o positiva. Algunos autores como Norberto Bobbio(1998:111) prefieren decir que es una libertad como ausencia de impedimento y una libertad como autodeterminación, en donde la primera representa la acción humana realizada sin obstáculos y la segunda simplemente la voluntad de hacerla decididamente. Esto se verá en la sección que trata acerca del principio general de la libertad.

¿Cómo se proyecta esto en el derecho a la intimidad? En primer lugar la intimidad como derecho es entendida como la libertad de un espacio privado, que se me reserva para mí y mi familia, donde puedo guardar todo de mí y compartirlo a unas pocas personas, quienes son las que pueden tener acceso, el llamado el “despliegue de la personalidad en la intimidad” (Zavala, 1982:24). En segundo lugar esta libertad despliega las dos caras del principio general: libertad negativa, que debe ser protegida celosamente por el estado al evitar que otros realicen acciones de intrusión y libertad positiva, permitida por la existencia de la intimidad, sin notorias influencias externas, lo que apoya el despliegue de todo el poder autónomo, que se proyectara en los cambios exteriores que hace el ser humano con su vida.⁵

⁵ Esta idea permitirá que la Corte Constitucional colombiana formule la existencia del derecho de protección de datos personales, entendiéndolo inicialmente como garantía de no intrusión en la intimidad, al respecto es patente lo afirmado por la Corte en sentencia T-414 de 1992: “(...) **la posibilidad de acumular informaciones en cantidad ilimitada, de confrontarlas y agregarlas entre sí, de hacerle un seguimiento en una memoria indefectible, de objetivarlas y transmitirlos** (...) permite un nuevo poder de dominio social sobre el individuo, el denominado poder informático. (...) **Como necesario contrapeso, este nuevo poder ha engendrado la libertad informática. Consiste ella 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. Es, como se ve, una nueva dimensión social de la libertad individual diversa, y por razón de las circunstancias que explican su aparición, de otras clásicas manifestaciones de la libertad. “(Subrayado fuera de texto)

Ante la necesidad de proteger esta libertad regulada en derecho, del dominio que estaba teniendo la sociedad, a las personas se les reconoce la capacidad de control sobre la información. Este derecho surge luego de un proceso histórico de modernización de las tecnologías que hace muy fácil, sencillo y económico tomar la información para tratarla de la manera más adecuada para tomar decisiones, pero esa información valiosa pertenece a personas que en cierta manera pueden verse afectadas. Una consideración generacional de los derechos humanos permite entender mejor cual ha sido el papel de la libertad como antecedente inmediato del derecho de protección, esto se examinará en la sección “Ubicación del Habeas Data en las Generaciones de Derechos Humanos”

Paralelamente, al reconocimiento de la libertad y el consecuente desenvolvimiento en principios concretos a unos determinados ámbitos de interés, el Estado comienza a transformarse desde un ente que debe estar totalmente cruzado de manos en la intervención de los derechos para no restringirlos, a uno Estado que se reformula totalmente a partir de dos hechos concretos: la preocupación por una igualdad real y la manera como puede lograrse.

El interés de lograr una mayor igualdad se justificó por la necesidad poder ejercer sin condicionamientos o afectaciones las libertades civiles. En vista que ejercicio defectuoso de unas libertades reconocidas formalmente se vinculaba a la gran desigualdad económica existente se propuso la manera como podía lograrse: I) en principio se pensó en un Estado más intervencionista de la economía para generar oportunidades que se denominó Estado Social de Derecho, pero luego también se miró desde la óptica jurídica, donde si bien se reconocían los derechos fundamentales en textos normativos superiores, faltaban instrumentos para lograr su efectividad rápida, sin que tuviesen que esperar al desarrollo del legislador y para mantener la superioridad normativa, en este aspecto, aparece el Estado Constitucional y Democrático de Derecho. Esto se explicará en la sección denominada “Transformaciones del estado de derecho”

Por la similitud en la raíz del daño causado en el indebido tratamiento de datos personales, la falta de consentimiento o autorización, con el derecho a la intimidad, se cree adecuado analizar el tipo de responsabilidad que es pertinente a este derecho para comprender

la que tengan los responsables, encargados y usuarios del tratamiento de datos personales ante la vulneración de los principios y obligaciones que tienen a su cargo. Esto se explicara en la sección “Afectación de las tecnologías a la intimidad”.

El principio general de la libertad

La libertad en sentido antiguo es entendida como una facultad de participación y ejercicio del poder político, en sus creencias y sus ideas, sin garantías para su ejercicio efectivo (Pérez Luño, 2005:111,112). La libertad en sentido clásico o griego significaba la satisfacción de la naturaleza propia de cada quien y ello implicaba encontrar el *telos* a través del uso del *logos* o entendimiento de todo lo que rodeaba al hombre. Costas Douzinas (2008:35 y ss.) lo llama teleología natural porque se intenta buscar el fin con la “observación de la naturaleza del cosmos, de las cosas y de los seres [sic] en él implica que se les impute objetivos, propósitos, fines políticos, siempre en conjunción con otras cosas y seres (...)” simplemente porque así se contribuye a perfeccionar el ser y desarrollar todo su estado potencial, en términos aristotélicos.

Esa teleología natural intentará buscar el *telos*, proponiéndolo como aquello que es permanente en medio de la diversidad (sofistas), el disfrute tranquilo de los placeres humanos, asociándose en la polis para lograrlo (epicureistas), la conservación de una tranquilidad para lograr la reflexión que permitía hallar la vida digna de ser humano común a todos (estoicos). Esta última idea de los estoicos influye en la concepción del derecho a través de la noción de normas racionales universales⁶, que entiende como el resultado de hallar las relaciones objetivas inmanentes al mundo mediante el *logos* voz interior que le revela, que denominaron derecho natural y que al tener tal carácter objetivo debían provenir de un ser superior.

Escuchar la voz interior vuelve el problema de la teleología natural a la persona misma. El hombre para ejercer su libertad ya no debe analizar lo que le rodea, sino pensar en sí mismo

⁶Esta necesidad de recurrir a principios universales es por la búsqueda de una fundamentación trascendente que legitime el ordenamiento jurídico sea obedecido; hay una conexión con principios divinos que compartió un iluminado. Posteriormente serán reemplazados cuando se imponga la ciencia racional, en principios morales que dan fuerza de validez al ordenamiento.

y encontrar aquello que está inscrito en su alma; el mundo romano le reconoce su propia personalidad jurídica con una norma (Pérez Luño,2005:113), aunque el Imperio romano, más exactamente el emperador, no renuncia de disponer sobre sus ciudadanos.

El individuo es resaltado como una representación de lo universal en pequeño, la suma de todos los individuos representan lo universal en conjunto, le dan contenido. Sin embargo, es visto aún como vinculado a la comunidad, a quien un soberano la gobierna. “Los súbditos no le dan al soberano un derecho o poder que él no posea, ellos simplemente renuncian a su derecho a la resistencia” (Douzinas, 2008:96), por esta razón los documentos de derechos los reconocen de manera muy limitada en cantidad, descripción y titularidad de ellos.“El nacimiento del hombre moderno y de los derechos individuales atraviesa la teología del escolasticismo católico, que descubrió los principios del derecho natural en la manera como Dios creó los seres humanos” (Douzinas, 2008:73 y Pérez Luño2005:113)

La concepción medieval al “crear al individuo”, como alguien absolutamente voluntario que tiende a realizar los designios de Dios, separa a la comunidad en personas, que ahora están en capacidad de escuchar lo que la divinidad quiere para su vida “El poder absoluto del individuo sobre sus capacidades, una prefiguración inicial de la idea de los derechos naturales, era el regalo de Dios para el hombre hecho a su semejanza” (Douzinas, 2008:74). Los derechos preexisten al pacto porque son el otorgamiento de un poder divino; se intenta garantizar por medio de pactos entre el soberano y los nobles feudales ciertos derechos de los súbditos, entendiéndose que preexisten al pacto (vienen de un ser superior), se pretende la no-vulneración (Heller, 2007:37). Posteriormente las libertades particulares y excluyentes se extienden a la mayor parte de la población.

El profesor Antonio Pérez Luño (2005:46) piensa que en realidad ese proceso de “(...) subjetivación del derecho natural (...)”, desconoce los contextos históricos tan importantes como la conquista de América por parte de los españoles, un hecho que abrió las puertas a pensar en el sustento jurídico para reconocer a esos otros seres humanos, con unos derechos básicos simplemente por serlo y las condiciones político-económicas de las colonias inglesas americanas que reivindican la existencia de unos derechos en cabeza de cada sujeto.

Sólo falta el golpe más importante, que se da con el reemplazo de la voluntad divina por la voluntad racional del hombre, “(...) pues se consideraban expresión del espíritu eterno que obra en el hombre, testimonios de la luz divina en el espíritu humano” (Pérez Luño, 2005:45), donde se reafirma que sólo los individuos existen y solo ellos tienen derechos. Eso concluye Costas Douzinas (2008:74) al decir que la “(...) celebración de una voluntad omnipotente e incuestionable fue tanto el preludio de la abdicación total del derecho divino como la piedra fundacional de la omnipotente soberanía secular (...)”.⁷

Más adelante en la Edad Moderna, se aterriza a los confines “mundanos” buscando lo que es esencial al hombre, a su ser y sus cualidades, sin que dependiera de las regulaciones normativas estatales (que representaba al ser superior a través del soberano monarca), aunque sin apartarse demasiado del *Dios de la razón*, el postulado central de las llamadas teorías iusnaturalistas⁸. Son los inicios de la lucha contra la omnipotencia del estado y la reafirmación del principio de la libertad⁹, este principio sólidamente formulado surge como resultado de las reflexiones filosóficas que realizaron los pensadores de la escuela iusnaturalista para fundamentar un derecho natural inmutable, autónomo y universal en la razón, que solo el individuo debe reconocer y obedecer; era imprescindible que se le respetara porque le pertenecía al hombre para ejercer diversas facultades potenciales propias como ser humano. Su consagración jurídica-positiva vendrá después, con las declaraciones de derechos durante los siglos XVI, XVII o XVIII:

“Así, en el párrafo primero de la Declaración de Derechos del Buen Pueblo de Virginia de 1776 se lee que todos los hombres son por naturaleza igualmente libres e independientes, y tienen ciertos derechos inherentes (*inherent rights*), de los cuales, cuando entran en estado de sociedad (*into a state of society*), no pueden, por ningún acuerdo, privar o despojar a su posteridad. En la misma línea proclamaba el artículo

⁷En el mismo sentido se pronuncia Heller (2007:159): “(...) el reino del desarrollo de las energías humanas para fines propios que el hombre se pone a sí mismo.”

⁸Estas teorías consideran diversos aspectos de la realidad como permanentes o universales y que el derecho representa simplemente un proceso declarativo de las mejores normas de convivencia social, descubiertas por medio de la razón, para darle protección clara. Ver Pérez Luño, A. (2005) *Derechos humanos, estado de derecho y constitución*. Madrid: Tecnos. P.56-58 y 117-119.

⁹Dice al respecto Costas Douzinas(2008:78): “*Es profundamente placentero para un jurista, inmerso en la doctrina del contrato, creer que las formas legales y los acuerdos libres reposan en la base de la sociedad*”

segundo de la Declaración francesa de los Derechos del Hombre y del Ciudadano de 1789 que la meta de toda asociación política residía en la “conservation des droits naturels et imprescriptibles de l’homme”. (Pérez Luño, 2005:57)

Enmarcado el pensamiento legal en principios racionales los filósofos más destacados al respecto, como Locke y Hobbes por representar posiciones distintas, fundamentan la manera más adecuada para una protección de esos derechos que garantizan la libertad.

Para Hobbes el estado de naturaleza es igual a una guerra constante entre los hombres por imponer su voluntad y para Locke el Estado de guerra es sólo una perturbación del Estado de naturaleza que es de mera paz¹⁰. Ambos parten del supuesto que el hombre abandona el Estado de naturaleza para conformar una asociación civil, que encumbra una autoridad común a la cual entregan un poco de la libertad, de actuar cada uno como desee, bajo el interés de que se les permita realizar – Hobbes- o conservar – Locke - su vida en paz y seguridad.

Sin embargo Locke se diferencia en que fundamentará la necesidad del Estado de Derecho para preservar el cumplimiento de la ley natural, que impone ciertos deberes y derechos, pues es más fácil que uno sólo pueda ejecutar los derechos de resarcimiento y castigo por violar la ley natural a que lo haga cada uno por su cuenta (Locke, 1991:21 cit. por Cortés, 2010:109); el incumplimiento de la ley natural se produce porque los hombres son seres bastante irracionales a veces (Locke, 1991:13 cit. por Cortés, 2010:106) y en otras ocasiones algunos no explotan con su trabajo las habilidades, dadas naturalmente. “Tal es el derecho y nacimiento del poder legislativo y ejecutivo, así como de los gobiernos y sociedades mismos” (Locke, 1991:127 cit. por Cortés, 2010:119). Esta será una idea importantísima para la filosofía jurídica posterior, en especial el surgimiento de los Derechos Humanos, siendo el sustento del liberalismo que se proyecta en el Derecho con la creación de instituciones y herramientas que permitan protegerlos.

¹⁰Así lo afirma Cortés,2010:109): “En el estado de naturaleza es siempre posible que agentes libres y racionales terminen violando la ley y que la persona a la que se le ha confiado la administración de la justicia juzgue de forma arbitraria.”

El liberalismo político tiene su aporte fundamental para cambiar la concepción medieval y muchos filósofos aportaron sus ideas para desembocar en la teoría liberal de John Locke¹¹, cuyo rasgo más diferencial fue que fundamenta los derechos “(...) en el mero hecho de que la razón los considere inherentes a la propia naturaleza humana”¹² (Pérez Luño, 2005:117), principio de igualdad y libertad en el hombre que hace digno. Esto transforma el pensamiento legal, de una orientación divina y absoluta a las contingencias del individuo, quien además de poder hacer, tiene ahora la posibilidad de exigir que se respeten esos poderes y no sean excesivamente limitados por leyes¹³; la razón instrumental extiende su poder sobre todos los campos, desde las ciencias naturales hasta las sociales, en especial la moral y el derecho; se va a entender que la libertad de cada individuo sin límites puede ser peligrosa y que se hace necesario lograr un correcto ejercicio de la libertad que permita la autoconservación y el nuevo derecho centra el análisis en el contrato social que unifica las características e idiosincrasias individuales, comunitarias y nacionales en unos acuerdos comunes, del cual se deducen todas las reglas para la convivencia segura. Esto lo resume de una manera bastante metafórica Costas Douzinas (2008:87 y ss.) como una confrontación entre la razón y el deseo, donde el primero “(...) debe o reconocer su impotencia o tratar de reclutar las pasiones en su beneficio”, en este caso la razón se toma por el nombre de toda la comunidad en su búsqueda de lo último mencionado.

Los filósofos más destacados en sus planteamientos son Jonh Locke, Jonh Stuart Mill y Benjamin Constant, ellos concibieron los fundamentos filosóficos del derecho a la intimidad, pero fue Isaiah Berlin quien influyó bastante en el derecho a la intimidad con la formulación

¹¹Por ejemplo Thomas Hobbes que en su Leviathan pone el ejercicio de la libertad como el desarrollo de un derecho natural que no cuenta con impedimentos externos, salvo aquellos que sean destructivos o dañosos para la propia vida de quien los ejecuta (Hobbes, Leviathan cit. por Douzinas, 2008:84).

¹²Sin embargo algunos estudiosos modernos consideran que fijar la inmutabilidad y trascendencia de la razón como eje de los derechos fundamentales y humanos es una rica paradoja porque en cada momento de la historia se ha echado mano de la razón trascendente y de la naturaleza humana inmutable para resistir a los embates del estado, aunque a la larga se demuestre que estaba atado a la voluntad del momento.(ver Douzinas,2008:26 y ss.)

¹³Aunque lo que hace Locke es retomar los planteamientos de la filosofía griega acerca del carácter normativo de la naturaleza para determinar lo que es cada ser y como pueden hallarla a través del uso de la razón. Al respecto se encuentra en el libro del profesor Costas Douzinas una afirmación acerca de que la “(...) ley civil y los derechos son la versión secular de la ley natural. Su fuente sigue siendo la misma, una razón natural adaptada sólo a las exigencias del mundo secular; pero las necesidades prácticas de la vida civil frecuentemente conducen a órdenes que contradicen el derecho natural.”(Douzinas, 2008:93)

de los dos aspectos de la libertad. En síntesis conjunta de ellos, puede decirse que, partieron del análisis que implicaba el fin de la servidumbre junto a la limitación de los poderes monárquicos y la relación libre que establecía el campesino con su patrón o el trabajador con el dueño de la fábrica; concibieron la necesidad de un espacio donde todas las personas pudiesen estar sin la intervención estatal, esta idea representó el inicio del derecho a la intimidad como una prohibición de que el Estado entrase en ese santuario reservado. De este derecho se desprenderá con el derecho a la protección de datos personales.

El derecho a la protección de datos personales tiene su origen en el principio general de la libertad, porque representa la evolución del poder de hacer las cosas ante la invasión de la tecnología en nuestra voluntad, generando que el sujeto autónomo kantiano se destruya ante las grandes capacidades de influencia en nosotros, que se obtiene del tratamiento de la información. Para conservar la libertad se necesita la ampliación de las facultades de decisión acerca de quien conoce aspectos de nuestra vida y quien puede divulgarlos a terceras personas, para que así la intimidad, en un primer momento, convertirse en un poder vigilante del poder informático que trata de conocer todo y luego se vuelva el derecho a la protección del dato personal, de esa pequeña parte de nuestro ser.

El derecho de la protección de datos personales, como un derecho para el ejercicio de otros derechos, permitiría el ejercicio activo de las facultades o poderes en el ámbito social que corresponden a cada uno de estos. También es entendido como un derecho en sí mismo, que permite el ejercicio de las aspiraciones más profundas sin una determinación externa, en este sentido una garantía instrumental que sería la negación de la negación, es decir, la negación de aquello que nos determina a través del uso de nuestros datos personales hacia una dirección predeterminada.

El carácter compuesto del derecho de protección de datos personales permite afirmar que en esencia protege el ejercicio de la libertad en sus dos sentidos, positivo y negativo, lo cual hace prudente explicar a continuación en qué consisten estos dos aspectos de la libertad.¹⁴

¹⁴ Que resume de la siguiente manera el profesor Antonio Perez Luño (2005:152): "Isaiah Berlin ha resumido con precisión el alcance de la diferencia entre: la libertad negativa (*liberty from*), entendida como falta de impedimento externo,

a) Resistencia al poder externo: Libertad Negativa

El principio general de la libertad en su lado negativo, de no imponer limitaciones jurídicas a los individuos no fundadas en una ley (Del Vecchio, 1971:86) que el profesor Norberto Bobbio (1998:97) formula como “(...) la situación en la cual un sujeto tiene la posibilidad de obrar o de no obrar, sin ser obligado a ello o sin que se lo impidan otros sujetos”. Esta libertad tiene el principal rasgo de permitir, con las mínimas limitaciones, que las personas actúen cualquier ámbito de su vida a iniciativa propia¹⁵, por lo cual cada uno de los derechos que conocemos, como políticos y civiles, implican el desarrollo para un ámbito más concreto de la libertad general como principio. Por esta razón es el germen del desarrollo primigenio del derecho a la intimidad o privacidad, porque consiste en una garantía de abstención del Estado a no molestar a las personas lo menos posible su ámbito de la vida privada, regulándose las excepciones habilitantes por la ley.

Los planteamientos iniciales ayudaron a definir el desarrollo jurídico de la intimidad o *privacy* que proponen Brandeis y Warren como un derecho a estar solo (*right to be alone*) de intervenciones del estado y de cualquier persona, el derecho a la intimidad toma un marcado carácter absoluto al establecer en el Estado el deber de promover su respeto por todas las personas; la concepción de Warren y Brandeis tuvo la intención de mantener a raya a los medios de comunicación de la vida personal de uno de ellos, quien se iba a casar prontamente con una mujer, perteneciente a una influyente familia.

El planteamiento inicial de la intimidad como una “tutela jurídica de la soledad frente al Estado y otras personas” implica la siguiente gran pregunta ¿Qué aspectos cubre el derecho a la intimidad? Y ¿Cuáles son las conductas que deben abstenerse de realizar las personas

como ausencia de opresión, o como garantía de no intromisión del poder en las actividades privadas; y la libertad positiva (*liberty to*), que implica la posibilidad de ejercer activamente determinadas facultades o poderes, o de participar en el proceso social y político, o de disfrutar determinadas prestaciones. El profesor Norberto Bobbio (1998:110) se expresa en forma crítica frente al sentido de que se le adjudique la libertad negativa como *freedom from* y la positiva como *freedom to*. En este Benjamin Constant considera que la libertad del disfrute privado corresponde a la libertad en sentido negativo y como libertad de participar en el poder político la libertad positiva (Bobbio, 1998:114)

¹⁵ Está incluida de manera más amplia la libertad negativa si se entiende el hacer como el no hacer y “(...) puede obrar porque no hay ninguna norma que imponga la acción que él considera deseable (...) puede obrar porque no hay ninguna norma que imponga la acción que él considera no deseable” (Bobbio, 1998:98)

cuando tratan datos personales? Respecto a la primera pregunta, se tiene la respuesta de que actualmente la intimidad cubre además de los aspectos de la parte privado, también mayoritariamente aspectos sociales o mejor, proyecciones de nuestra identidad y nuestras acciones en la sociedad actual, identificar las conductas que afectan esas acciones permiten encontrarla respuesta al segundo interrogante, quienes reciben y conocen aspectos de nuestra vida personal, de esas proyecciones de nuestro espíritu, están limitados en lo que hagan con lo que conozcan a través de los principios de administración y tratamiento de datos personales, que reconocen de manera estándar las normativas internacionales y la ley estatutaria de protección de datos personales de Colombia.¹⁶

b) Respeto a la Autonomía Individual: Libertad positiva

La libertad en este sentido es la voluntad de hacer las cosas sin que directamente haya una influencia que sea el gatillo lanzador hacia esa decisión. Todo aquello que fuera “racionalmente indeseado” permitiría que se resuelva el contrato y se rebele contra el gobierno. Porque el hombre así como en su estado de naturaleza es libre, también en sociedad conserva la libertad para decidir las consecuencias razonables que desea y para romperlo cuando le son afectadas o no se presupuestó, todo en ejercicio de la autonomía como sujetos pensantes. “Lo correcto, que ya no se da objetivamente en la naturaleza ni en el mandamiento de la voluntad de Dios, sigue la razón humana y deviene subjetivo y racional. El derecho se transforma en derechos individuales” (Douzinas, 2008:75)

Lograr la resistencia a lo que nos impide ejercer nuestro derecho es lograr hacer justicia. Este es el núcleo fundamental del derecho natural clásico y es lo que permanecerá latente en las formulaciones iniciales del derecho a la intimidad como un *right to be alone* y luego despertara de su letargo, para exigir un papel cada vez más activo en el flujo de información que se conoce de nosotros, la manera como se usa esa información y la imagen generada de

¹⁶ Cuando no sean cumplidos estos principios de administración, nuestra libertad de obrar se encontrará tremendamente limitada por las valoraciones que hayan concluido otras personas que conocieron la información confidencial o la información falsa o inexacta.

nosotros ante el Leviathan moderno (el estado y las empresas multinacionales) y los otros miles de individuos. En estos términos lo afirma Costas Douzinas (2008:81): “El Derecho natural original, que postula la voluntad libre de acuerdo con la razón, fue el primero en reclamar la justicia que puede alcanzarse sólo a través de la lucha; no entendía a la justicia como algo que viene de arriba y le prescribe a cada uno su parte, como distribución o retaliación, sino como una justicia activa de abajo, aquella que haría la justicia misma innecesaria. El derecho natural nunca coincidió con un simple sentido de justicia.”

La libertad reconoce que podemos comprometernos en conjunto varios individuos, que terminaba en la conformación de un estado (entendido en el sentido del sujeto autónomo que reconoce las leyes del estado porque a ellas dio consentimiento previo en ejercicio de su autónoma facultad, ver Bobbio, 1998:101-102). El pacto contractual representaba una gran versatilidad porque permitía regular el orden, garantizando facultades individuales y al mismo tiempo dando pautas de convivencia en comunidad. Frente al individuo y al Estado bastaba oponer ese complejo sistema de reglas entero y – presuntamente – sin brechas para que la libertad positiva se mantuviera indemne.

Modernamente es llamada libertad positiva, se define como el ejercicio de nuestra autonomía, sin las presiones conscientes o inconscientes del medio. Se define como la autodeterminación, frente a lo cual el profesor Norberto Bobbio(1993: 101) afirma que “(...)se suele llamar “libertad” también a esta situación, que podría llamarse de manera más apropiada “autonomía”, en la medida en que la definición se ha hace referencia no tanto a lo que hay cuanto a lo que falta, como cuando se dice que autodeterminarse significa no estar determinado por otros, o no depender para las propias decisiones de otros, o determinarse sin ser determinados”.

Este concepto de ejercicio de la capacidad autónoma se relaciona profundamente con el imperativo kantiano que permite afirmar la facultad de acatar las regulaciones externas sobre la base de que las hubiese podido haber aprobado. Este imperativo kantiano que incentiva el respeto al ser humano permite salvaguardar su dignidad humana, afirmar que de cada hombre no se puede esperar que trate a los demás de forma instrumental, sino como fin en sí mismo.

La precisa afirmación obtenida apoya la independencia del derecho de protección de datos personales de la intimidad, al concebirlo como un derecho a la autodeterminación informática, como una facultad reconocida al usuario para ejercer un control activo sobre el flujo de información en la sociedad que concierne sobre él.

c) La formulación práctica del derecho a la intimidad como desarrollo del principio general de la libertad

La teoría del abstencionismo de Estado deriva del principio general de la libertad en sentido negativo, se flexibiliza ante la necesidad social de ceder parte de los derechos individuales para lograr la convivencia humana. Precisamente la colectividad obliga a las personas a ceder su absoluta libertad.

Como bien se ha visto en las dos secciones anteriores, la libertad negativa implica la garantía de que habrá una ausencia de impedimentos para poder hacer las cosas, el derecho a la intimidad vendría siendo una libertad negativa de las otras personas para que tengamos la garantía de respetarse nuestro espacio privado. Pero al mismo tiempo nos permitirá, en su aspecto positivo, ejercer nuestra potestad dentro de esta gran espacio privado y social que proyectamos y sólo , podremos reservarlo a nuestros asuntos que conciernen a la familia y nuestra individualidad, sobre todo será reflejo de nuestra absoluta identidad y nosotros estaremos habilitados para decidir a quién dejamos entrar o no.

Es requisito indispensable que ambas libertades se coordinen mutuamente; existiendo una serie de normas claras acerca de las limitaciones y facultades que puede ejercer cada uno, puede fácilmente deducirse cuando se está impidiendo el ejercicio de ellas, por ende también podrá entenderse que se quiere estar determinando el querer o la autonomía. Por lo anterior puede afirmarse que en general todo impedimento ejecutado significa un interés profundo en determinar la voluntad hacia una dirección específica. Esta última conclusión será el soporte fundamental para deducir el sistema de responsabilidad civil aplicable a los encargados, responsables y usuarios de datos personales por vulneración de las normativas estatutarias de

protección de datos personales, que se verá en la sección sobre la afectación del internet al derecho a la intimidad.

La ubicación del Habeas Data en las generaciones de Derechos Humanos

La libertad es el germen de todos los derechos humanos, incluso de los otros principios hermanos que son la igualdad¹⁷ y la dignidad¹⁸ (Alexy, 2007:311), porque a través de su limitación o ampliación se incide en los segundos. Por ejemplo, la dignidad se limita cuando se restringe una acción para conseguir las profundas aspiraciones de cada persona, de tal manera que se resalta el valor intrínseco, “(...) ser restringido arbitrariamente en la libertad, es algo que contradice la dignidad humana (...)” (Alexy, 2007:314); la igualdad puede ser impedida, sin argumento justificado claro, cuando no se dan las oportunidades a algunos, pero a otros sí, que permiten materializar las aspiraciones perseguidas (igualdad).

En sentido jurídico los derechos humanos son usados de tres maneras: a) como contención ante el avance del Estado Absoluto, b) como argumento por las personas marginadas que los reivindicán y c) como una garantía de inmutabilidad y protección ante cualquier intervención estatal; los usos de los derechos humanos permiten deducir su carácter de universalidad (valen en cualquier lugar y momento), de validez moral (justifican la protección de ciertos intereses) y prioridad (deben tenerse presentes al momento de ejercer cualquier acto de autoridad), esto porque representaban los valores más estables de la naturaleza humana, y el interés de la positivización para intentar darles mayor eficacia jurídica (Peces-Barba, 1986:242). Al respecto dice el profesor Gregorio Peces-Barba (1988:272):

¹⁷Respecto a la igualdad se afirma que es de gran importancia para fundamentar los derechos sociales actuales que propenden por que la mayor parte excluida acceda a unas condiciones materiales básicas.

¹⁸La destaca el profesor Antonio Pérez Luño (2005:51) para afirmar la dimensión moral de la persona porque “(...) la idea de *dignitas* del hombre, como ser éticamente libre, parte todo el sistema de derechos humanos de Samuel Pufendorf, que, a su vez, fue fermento inspirador de las declaraciones americanas”

“El fundamento de los derechos humanos es la realización de esa función de la libertad social-política y jurídica como cauce del desarrollo de la dignidad humana que supone el dinamismo de la libertad de elección a la libertad moral”

La función de positivización de la libertad se ha manifestado, en múltiples intentos a través de los años, desde aquél siglo XVIII con las declaraciones de derechos iniciales, a favor del individuo y luego del ser humano sin distinciones, que aparecieron al calor de los hechos que surgían. Todas las corrientes filosóficas y políticas han sido, parafraseando a Ortega y Gasset, “ellas y sus circunstancias”, profundamente sensibles a la historia de su época¹⁹

Por esta dependencia histórica se propuso clasificar²⁰ los derechos humanos en generaciones, agrupando cada generación a partir de un hecho social que impactó en su consagración política y jurídica. Así, la primera generación de los derechos humanos estuvo marcada por el interés de las revoluciones burguesas del siglo XVIII de configurar las libertades individuales, que el estado no debe perturbar sino tutelar; la segunda generación, influida por las luchas obreras, femeninas y sociales marcan la pauta para configurarlas como libertades en sociedad, que permiten a las personas lograr una participación real; la tercera generación de los derechos humanos ha visto la luz a partir de las perturbaciones que afectan a las libertades individuales las nuevas tecnologías (Pérez Luño,2006:28).

La necesidad de separar los derechos en una tercera generación, se debe a que estos derechos son del tipo instrumental, pues tienen la tutela de un interés jurídico diferente, a través de ellos se permiten garantizar con certeza que se respeten los derechos individuales, por ejemplo, la llamada libertad informática o Habeas Data al reconocerse como el derecho al control de la información personal que está almacenada en las bases de datos representa un alivio para que las personas puedan conocer cuando se presentan vulneraciones de derechos conexos como la intimidad, el buen nombre, el honor, la honra, el uso de la imagen personal. “Ya que en efecto cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida, que afecta potencialmente incluso aspectos más sensibles de

¹⁹En este sentido ver Pérez Luño, 2005:93 y ss.

²⁰Quien primero lo hizo fue Paul Vasak en su conferencia inaugural en el Instituto de los Derechos Humanos de la ONU

su vida privada; aquellos que en épocas anteriores quedaban fuera de todo control por su variedad y multiplicidad” (Pérez Luño,2006:31)

Tal preocupación se tomó en serio cuando la información adquirió tal importancia que nuestras sociedades actuales de denominan “sociedad de la información”, en virtud de las potentes capacidades de la informática y las nuevas tecnologías para analizar grandes cantidades de información personal y luego tomar decisiones comerciales, gubernamentales, sociales, económicas, criminales. Incorporar la concepción generacional de los derechos humanos ha permitido el surgimiento de nuevos derechos al evitar la taxatividad que anquilosa el ordenamiento jurídico a lo planteado hace siglos e ignora que las nuevas necesidades humanas claman por el reconocimiento de unos nuevos derechos y la instrumentalización de los medios para protegerlos.²¹

Transformaciones del estado de derecho

La teoría liberal de John Locke, propuesta en su “Segundo Tratado sobre el Gobierno Civil”(2006) , es la base inicial de la preocupación del derecho por el ser humano de protegerle sus bienes básicos y respetar la naturaleza racional del hombre ; el presupuesto fundamental es la necesidad de conservar parte de la libertad del estado natural cuando se asocian para superar el estado de guerra y también darse una autoridad común que conserve la protección de los bienes, porque se ve expuesta a la vulneración por defensa excesiva o por agresión inminente(Cortés, 2010:103), lo cual merma las potencialidades y aspiraciones de vida. Esta autoridad común es la designada para resolver esas agresiones que son fuente de conflictos y decidir el castigo a los que perturban, así lo señala Locke(2006:87):“Aquellos que están unidos en un cuerpo y tienen establecida ley común y una judicatura a la que apelar, con autoridad para decidir entre las controversias y castigar a los ofensores, forman sociedad civil”

²¹Al respecto opina el profesor Pérez Luño(2005:85) sobre las transformaciones de los derechos humanos al ubicarlos históricamente anclados a las reivindicaciones del momento: “Principios originariamente dirigidos a poner límite a la actuación del Estado se han convertido en normas que exigen su gestión en el orden económico y social; garantías pensadas para la defensa de la individualidad son ahora reglas en las que el interés colectivo ocupa el primer lugar; enunciados muy precisos sobre facultades que se consideraban esenciales y perennes han dejado paso a normas que defienden bienes múltiples y circunstanciales”

Es la idea de la formación contractual del estado, donde todos se asocian porque es más beneficioso que seguir en el estado de naturaleza, que muchos filósofos interpretaban en diversos sentidos como “(...) competitivo y agresivo, para otros pacífico y laborioso, para otros ambas cosas.”(Douzinas, 2008:77); todos los intentos buscaban encontrar algo regulador y común a toda la humanidad, finalmente se decantan por la razón unida a la teoría del contrato social, de esta manera se justificaba la necesidad del estado y se evitaba caer en el extremo individualismo, de las iniciales teorías liberales, que imposibilitaba la convivencia social(Douzinas, 2008:77) porque la“(…) sociedad civil nace sólo por el consentimiento y tiene por finalidad principal garantizar mediante leyes positivas que expresan el sentir de la mayoría de los representantes del pueblo [sic] la vida, la libertad y los bienes de los asociados.”(Pérez Luño, 2005:118). Recordemos las declaraciones de Virginia, la Carta Magna inglesa, la Declaración francesa de 1789 que intentan llevar a normas un conjunto de puntos acordados por representantes a nombre del pueblo. Pérez Luño (2005:121) concluye que:

“A partir de entonces se inicia un proceso de progresiva relativización del contenido iusnaturalista de los derechos fundamentales, los cuales pasan a encuadrarse en el sistema de relaciones jurídico-positivas entre el Estado, en cuanto a persona jurídica, y los sujetos privados, que la dogmática alemana del derecho público estudiará bajo el epígrafe de los derechos públicos subjetivos”

a) Estado formal de derecho

La tesis acerca del origen del Estado de derecho se debe a Inmanuel Kant, quien afirma ser una necesidad para conservar la libertad individual y la libertad de participación (Pérez Luño, 2005:223). Esta última que no puede ser eliminada al crearse el estado, solamente es delegada a un legislador común, quien formula normas vinculantes a toda la comunidad bajo el presupuesto de que así lo hubiese hecho cada miembro, de manera individual en ejercicio del imperativo categórico. Al respecto afirma el profesor Pérez Luño que Kant: “Ayudado por la idea de contrato social, que permite aglutinar a todas las personas con el ideal de un solo

legislador que hubiese expresado la voluntad conjunta del pueblo. Lo que el hombre pierde con el contrato social es su libertad natural y un derecho ilimitado a cuanto le apetezca y pueda alcanzar; lo que gana es la libertad civil y la propiedad de todo lo que posee.”(Pérez Luño, 2005:222)

El estado de derecho inicialmente consagra garantías *formales*, como el respeto a la ley, la división de poderes y los procedimientos fijados para expedir una norma; se legitimaba *materialmente* en la medida que la actividad estatal respetara la estructura institucional y jurídica que había emanado del poder soberano popular, representado por el legislador, para rescatar los derechos de los individuos de la arbitrariedad política de los gobernantes. Sin embargo con el énfasis en el absoluto respeto a esas garantías *formales*, genera la percepción de que el Estado sea entendido como Derecho y su actuación se limite a “(...) garantizar jurídicamente el libre juego de los intereses económicos” (Pérez Luño, 2005:228).

Los orígenes del Estado de Derecho se alimentan del principio de legalidad, que a su vez es sustentado en la idea de formularse unas normas, racionalmente creadas, para regular los derechos que encauzan el ejercicio de la libertad por parte de las personas.

Los derechos fundamentales son el motivo indirecto para la formulación del tipo de Estado, al ser su eje principal la regulación positiva de unas posiciones jurídicas, que se consideraban importantes respetar para todo hombre o ser humano porque le permiten ejercer su libertad, en términos kantianos. Esto ocurre en el momento en que el positivismo filosófico se ha tomado el derecho, para eliminar cualquier resquicio de iusnaturalismo, inclusive cualquier clase de referencia a derechos naturales inherentes al ser humano²², por esta razón intenta convertirlos en derechos reconocidos por el Estado²³, frente a los cuales tiene el deber respetar y garantizar que otras personas no los vulneren. De esta manera los ciudadanos se convierten en sujetos pasivos, a quienes se les concede una serie de prerrogativas, que puede

²²El Estado es la única fuente de derecho permite relativizar cualquier derecho surgido antes o que fuese inherente, lo cual vuelve a los derechos naturales y fundamentales con dos opciones: ser olvidados o ser simplemente una norma reconocida de acuerdo a los principios de validez. Esta última posición cerrada hará difícil que el Estado se adapte a las variaciones sociales y se solidifique hasta el punto de entrar en crisis.

²³ El profesor Pérez Luño (2005:59 y 248) concluye que “En efecto, la nueva categoría se presentará como intento de ofrecer una configuración jurídico-positiva, de la exigencia mantenida por la teoría de los derechos naturales de afirmar las libertades del individuo frente a la autoridad del Estado.”

reclamar al Estado debido una relación jurídica previa y que reconoce pretensiones denominadas en términos de Jellinek como derechos públicos subjetivos, en contra de aquellos derechos subjetivos que se crean al amparo de la autonomía de la voluntad. Esos derechos públicos subjetivos se incorporan al derecho constitucional liberal desde el derecho administrativo del siglo XIX, que los concibió como “(...) derechos de los ciudadanos que marcaban el límite de la actividad del Estado-administración y cuya vulneración, por parte de este último, hacía surgir pretensiones judiciales dirigidas a su restablecimiento” (García de Enterría, E. y Fernández, T., 1993:17-101 cit. por Osuna, 1998:84)

La formulación acerca de la existencia de derechos públicos subjetivos implica tres aspectos importantes: i) la preeminencia del estado como fundamento del derecho, ii) la necesidad del derecho, en concreto de la ley, para conservar el orden y iii) El reconocimiento de la personalidad jurídica del Estado, necesaria para garantizar que tiene obligaciones a cargo y derechos a su favor frente a los ciudadanos.

Una institucionalidad fuerte para la tutela de derechos, unas normas claras que lo reconocen y un ciudadano sujetado a estos dos aspectos son el culmen del Estado de Derecho; la relación del Estado de Derecho con los Derechos Fundamentales entra en escena y estos últimos comienzan a estar adscritos a posiciones jurídicas reconocidas por el Estado. Así puede apreciarse en la siguiente idea del profesor Pérez Luño (2005:59)

“Para eso se precisaba de unas estructuras del poder de forma que fuera posible la instauración de relaciones jurídicas entre el Estado y los particulares, para lo que se debía reconocer la personalidad jurídica del Estado, que de este modo adquiriría la titularidad de derechos y obligaciones para con los ciudadanos, estableciéndose también una consiguiente tutela jurisdiccional de las situaciones subjetivas así instituidas” (Pérez Luño, 2005: 59)

Las características del Estado de Derecho están resumidas por el profesor Ernst Böckenforde (2000:19) en tres elementos: a) El estado sirve a una “comunidad” que se forma alrededor de los intereses comunes de las personas o igualdad ciudadana en la participación, b) El estado por lo anterior no debe intervenir más allá, en los intereses propios de cada uno,

debe antes bien eliminar los impedimentos que les surjan en el ejercicio de la libertad o autonomía civil, c) Para garantizar que la actividad del Estado cumple los fines comunes se expiden unas normas “racionales” que lo organizan y fijan el marco imperativo dentro del cual debe actuar.

Lo que es transversal a todo el Estado de derecho consiste en el interés de ordenar la convivencia social²⁴ a través de las leyes, que son vinculantes en la medida que recojan los postulados y aceptaciones de la voluntad racional de cada persona, en este sentido, la manera de lograrlo se justifica a partir de la soberanía popular que reside en el Parlamento o legislador democrático. Al respecto el profesor Ernst Böckenforde (2000:24) concluye que “(...) esta ley significa “el dominio del principio de la libertad de los ciudadanos del Estado” en la que se combinan “voluntad general y autodeterminación de los individuos”.

El Estado de Derecho luego se transforma en el factor potenciador del carácter vinculante de los derechos fundamentales, a través del ejercicio de la función jurisdiccional de control constitucional.²⁵ Consecuentemente se han ido asociando entre sí, hasta el punto de no concebirse el uno sin el otro, debido a que en el momento contemporáneo actual se utiliza para explicar la noción de una estructura jurídico-política del estado que intenta cumplir ciertos fines sociales.

b) Estado social de derecho

En el plano jurídico, los esfuerzos del Estado de Derecho por aferrarse al orden²⁶, entendido como preservación de la legalidad a través del control jurisdiccional de los actos de la administración (Pérez Luño 2005:229) y la ejecución de la ley asignada a una estructura

²⁴Esta convivencia social implica que el ejercicio individual de los derechos no perjudique a los demás en su libertad.

²⁵ El profesor Pérez Luño (2005:219) coincide con esta afirmación al expresar que “(...) cumplen una misión de fundamento y límite de todas las normas que organizan el funcionamiento de los poderes públicos, y, en suma, de todas las experiencias concretas de juridicidad surgidas en el seno del ordenamiento en que se formulan.”(P.219)

²⁶Algunas de las definiciones de Estado de Derecho que adjudica Erns Böckenforde (2000:26-28) que tienen el elemento de orden, del cual se deduce la necesidad de estructura institucional y norma legal o superior así: para tener orden se requiere expedir normas válidas que están señaladas en la norma constitucional y que para ejecutarse se precisa de una estructura que permite conservar el orden. Todos implicados mutuamente

administrativa competente (Böckenforde, 2000:30), comienzan a ser permeados por las presiones que surgen de garantizar la libertad, la igualdad reales y la participación democrática reales. Los anteriores derechos eran reconocidos en las Constituciones de los países, pero no se materializaban en la vida cotidiana para la amplia mayoría de ciudadanos (Böckenforde, 2000:35)

Ese estado de miseria se intensifica después de la Segunda Guerra Mundial y el Estado comienza a ser interventor y generador del crecimiento económico para toda la sociedad con el fin de garantizar la existencia material básica, que permitiría la convivencia y el disfrute de los derechos civiles a través del reconocimiento de nuevas prerrogativas fundamentales; los derechos fundamentales ahora plenos de contenido dan la orientación a la actividad estatal para proyectarse realmente en la sociedad.

Esta época va en consonancia con la segunda generación de los derechos humanos, preocupados por tutelar aspectos de la personalidad que se desenvuelven en medio de la sociedad, con el otro y para el otro. (Ver al respecto Supra La ubicación del Habeas Data en la Generaciones de los Derechos Humanos). Este nuevo tipo de estado implica una “(...) fórmula de compromiso entre la defensa de las libertades tradicionales de signo individual y las exigencias de justicia social”, por la confluencia de estos dos aspectos se denomina Estado Social de Derecho. (Benda, 2004:526).²⁷

Es esencial que se mire al individuo en sociedad como al individuo en soledad, que en conjunto todas tengan acceso a un mínimo de bienes materiales y oportunidades²⁸, y que a

²⁷Al respecto merece destacarse lo planteado por Pérez Luño(2005:230-233): “El estado social de derecho tuvo, por tanto, un origen híbrido fruto del compromiso entre tendencias ideológicas dispares, que ha gravitado sobre su evolución ulterior.(...) Su componente socialista democrática se traduce en la superación del agnosticismo axiológico y del formalismo positivista al imponer al estado la realización de determinados fines materiales, que contribuyan a una reforma social y económicamente justa, en términos de justicia social, de las condiciones de convivencia(...) La impronta liberal tiene su manifestación más precisa en las tesis de Keynes, principal inspirador del *Welfare State*, que defendían la posibilidad de una transformación de la política estatal por vía democrática y respetando la economía de mercado capitalista, así como el derecho de propiedad sobre los bienes de producción. Se acepta, sin embargo, un abandono del dogma *laissez faire* en favor de un intervencionismo de los poderes públicos en el proceso económico tendente a un incremento constante de la producción, que permita garantizar el pleno empleo y el aumento de las rentas de trabajo.”

²⁸ Resaltar la importancia de lo social lo refieren así el profesor Ernesto Benda (2004:536): “Al núcleo de lo que la cláusula del Estado social quiere garantizar pertenece la previsión social del mínimo existencial mediante la política social clásica” y el filósofo del Estado Hermann Heller (1942:101): “El punto de partida ha de ser aquí la fundamental e inmovible afirmación de que la realidad social es efectividad humana, es realidad efectuada por el hombre”.

cada uno se le respeten sus derechos fundamentales y posiciones jurídicas adquiridas; la confluencia de estas ideas garantiza el principio de la libertad en sociedad.²⁹ En este tipo de Estado el individuo debe ofrecer todo su esfuerzo para no depender en subsistencia del gobierno, ello atentaría contra su dignidad humana, su valor en sí mismo y le haría quizá esclavo de los subsidios que se entreguen, viéndose como una dádiva. Al mismo tiempo la intervención del Estado no se limita a los problemas económicos, también busca supervisar y promover soluciones a los problemas culturales y ambientales.

El Estado social de derecho si bien en principio se centra en la distribución del crecimiento económico busca que se puedan ejercer las libertades civiles, sin que los problemas sociales influyan en la autodeterminación de vida; reaccionar a los nuevos problemas que surgen con la tecnología y la integración económica global se convierte en un aspecto que influencia las políticas y normas jurídicas de este Estado.

Vale bien la pena mencionar los rasgos características del Estado social de Derecho según el profesor Antonio Pérez Luño (2005:233 y ss.): “a) la afirmación de la necesaria continuidad entre los principios social y democrático y el Estado de derecho. (...) b) (...) supone también el reconocimiento de la “abolición fáctica de la separación entre el Estado y la sociedad (...) c) (...) la superación del carácter negativo de los derechos fundamentales (...) de meros límites de la actuación estatal para transformarse en instrumentos jurídicos de control de su actividad positiva (...)”.

Estos rasgos los define en las siguientes nociones el profesor Ernesto Benda (2004:493 y ss.) al analizar la Ley Fundamental de Alemania: i) seguridad jurídica y justicia material³⁰, “El ciudadano debe conocer los márgenes a su disposición para configurar la propia existencia, y también saber que no puede atentar contra los derechos ajenos” y contra el derecho a la igualdad de trato sin fundamento, teniendo a su vez la expectativa de que serán útiles los

²⁹ “No se trata de disociar dos esferas que son de por sí distintas. Por contra, se plantean cuestiones urgentes tan pronto se trata de ordenar con sentido actividades que pueden realizar tanto el estado como la sociedad”(Benda:540)

³⁰A través de la reserva de ley mayormente el ciudadano guarda las expectativas acerca de los asuntos y procedimientos por los cuales puede limitarse su libertad. En opinión de Ernesto Benda (2004:502) le permite “anticipadamente (...) con qué reacciones del estado a su comportamiento debe contar (...)”

instrumentos jurídicos para cuando se atenten contra sus derechos; ii) Garantías vinculantes para la Constitución como norma suprema, “Una efectiva protección de los derechos fundamentales depende decisivamente sin embargo de que institución y con qué procedimiento puede juzgar sobre un atentado a la Constitución”; iii) vinculación de los poderes públicos al derecho, para todos ellos debe existir una estabilidad, que no haberla representaría una amenaza a la existencia del ciudadano y a sus derechos fundamentales, por eso la Constitución es la “idea-directriz del ordenamiento”, el legislador con un mayor margen puede actuar en sus decisiones al expedir las leyes sobre cómo desarrollar la Constitución³¹, los jueces pueden realizar la creación judicial dentro de sus márgenes, cuando existen lagunas de ley, fijando su postura según los valores de esta, poderes y la administración, con una potestad discrecional que tiene unos límites precisos de la ley; iv) división de poderes, implica una asignación especializada de funciones a las autoridades públicas sin que dejen de actuar coordinadamente³² y sin olvidar que a través “(...) únicamente el control y la limitación recíprocas de los órganos legislativos (legislativo, ejecutivo y judicial) produce la moderación del poder y protege la libertad individual”³³; v) protección de los derechos fundamentales, implica propender porque se respeten y se regulen procedimientos específicos para que el ciudadano que cree vulnerado sus derechos, acuse los actos jurídicos de la administración o las normas expedidas por el legislador³⁴; vi) Confianza jurídica, significa que

³¹ El legislador al expedir las leyes realiza todo un proceso político y democrático donde decide que una determinada manera de hacer las cosas es la correcta, esa decisión plasmada en la ley sobre un determinado asunto estará limitada, para que sea válida dicha norma, a unos parámetros fijados en la Constitución según el tipo de asunto tratado, esto se denomina reserva de ley, y permite el ejercicio del control judicial por el ciudadano que se crea afectado.

³² El profesor Pérez Luño atinadamente señala que modernamente se entiende como un principio de racionalización y colaboración ante los diversos enfoques de solución que enfrentan los órganos a los problemas sociales: “Gran parte de la doctrina y la jurisprudencia germana entiende que el principio tradicional de la división de poderes, según se recoge en la *Grundgesetz*, no debe interpretarse como exigencia de una rígida separación, sino como la de un control y colaboración recíproco entre todos los poderes que ejercen funciones estatales para lograr una coordinación armónica en sus tareas. Por ello, tal principio debe ser completado por el de subsidiariedad, en virtud del cual, cuando los órganos legislativos no asumen la tarea de desarrollar y completar positivamente las disposiciones constitucionales, tal tarea puede ser realizada por el juez” (Pérez Luño, 2005:106-107)

³³ Un ejemplo de esta colaboración armónica es el procedimiento de aprobación de las leyes estatutarias que establece la Constitución de Colombia de 1991, en el que intervienen el Congreso con el proyecto de ley, que remite a la Corte Constitucional colombiana para su enjuiciamiento conforme a la Constitución, si pasa el filtro, se remite al Presidente de la República para que la sancione, publique y promulgue.

³⁴ En este tipo de estado la protección de los derechos fundamentales se empieza a acentuar en los jueces, contrariamente al Estado de Derecho, donde el juez debía aplicar las normas generales que desarrollaban los derechos fundamentales, “(...) no le correspondían funciones creadoras y mucho menos en el terreno de las libertades fundamentales en el que el juez debía limitarse a aplicar estrictamente aquellas normas generales y previamente sancionadas en las que éstos venían promulgados.(...)” (Pérez Luño, 2005:106)

el Estado estimule frecuentemente la expectativa de protección y guarda del ciudadano a través de sus instituciones, cortando las leyes confusas, los trámites dispendiosos y los procesos largos para lograr obtener la tutela de sus derechos³⁵; vii) La re-configuración social a favor de los débiles y necesitados “(...) presupone la conciencia de que el *bien común* no resulta por generación espontánea” (Benda, 2004:526), en dicha labor el Estado no puede imponer cargas tan excesivas que limiten profundamente la libertad, si ocurre una colisión con esta es pertinente aplicar la ponderación, propuesta por Robert Alexy en su libro *Teoría de los Derechos Fundamentales*, como método para mirar la prevalencia de posiciones jurídicas.

c) *Estado social y democrático de derecho*

El Estado social de Derecho abre las puertas a una democracia plural que se encuentra limitada por unas estructuras institucionales a través de las cuales debe encauzarse y unos principios constitucionales supremos, representantes de unos valores prioritarios para el conjunto social, que deben respetar en su ejecución (Benda, 2004:490 y ss.) Es una necesidad remarcar los aspectos sociales y democráticos, este último olvidado dentro del Estado de Derecho, por las amenazas que puede traer la voluntad mayoritaria absoluta, pero que representa el beneficio de estar atento a las circunstancias cambiantes, “actualizando” el Estado Social de Derecho (ESD). En este punto la doctrina afirma que el ESD debe transformarse en el Estado Democrático y Social de Derecho.

Contemporáneamente, además de la inclusión del adjetivo democrático, recientemente dentro del Estado de Derecho, se ha resaltado que la Constitución debe ser la única ley superior, porque es el desarrollo de los límites de la libertad de las personas cuando se convive en sociedad a los que se ha vinculado los derechos humanos con la estructura estatal. Cuando la ley es referida a una norma superior, no como inicialmente se entiende que es esa norma

³⁵Más cuando en los momentos presentes por el pluralismo se están presentando distintas fuentes de producción normativa: “El desplazamiento del centro de gravedad en el proceso de determinación de las fuentes jurídicas no sólo se ha producido por la aparición de poderes normativos superiores al Estado, de forma paralela se ha producido una ampliación de competencias normativas por parte de los entes sociales intermedios, situados entre el ciudadano y el poder estatal” (Pérez Luño, 2006:53)

formal y general, que proviene de una entidad representativa de la soberanía popular, la Constitución otorga al Estado de Derecho la legitimidad político-jurídica necesaria para continuar operando de cara a sus ciudadanos; son el fundamento auténtico del Estado Democrático, Social y Constitucional de derecho. El profesor Peter Habermas afirma en consonancia con lo anterior que: “(...) el estado constitucional es un arquetipo jurídico-político en el que los poderes públicos se hallan conformados y limitados por el derecho a través de principios constitucionales formales y materiales: los derechos fundamentales, la función social de las instituciones, la división de los poderes y la independencia de los tribunales.” (Cit. por Pérez Luño, 2006:67). Los rasgos que reflejan esta transición los resume el profesor Pérez Luño (2006:53) en tres aspectos: i) El desplazamiento desde la primacía de la ley a la primacía de la constitución; ii) El desplazamiento desde la reserva de ley a la reserva de constitución; iii) El desplazamiento desde el control jurisdiccional de la legalidad al control jurisdiccional de la constitucionalidad”

El estado a través del protagonismo creciente de la jurisdicción constitucional y la justicia en general pretende que todos cumplan la ley constitucional. Al respecto Ronald Dworkin lo afirma así: “Si el gobierno no se toma los derechos en serio, entonces tampoco se está tomando con seriedad el derecho”³⁶ (Dworkin, 1977:303 cit. por Pérez Luño, 2006:26). Se enfatiza en la creación de nuevas herramientas para su tutela: acciones procesales especiales, ampliación de la competencia en las autoridades judiciales para conocer a través de las acciones vigentes y en las autoridades administrativas para defender los derechos a través de la facultad para imponer sanciones.

Afectación del internet a la intimidad de los individuos

A partir de los años cincuenta se inicia el proceso de interconexión mundial, esto significa que las personas van a comunicarse con más rapidez, la información va a fluir libremente entre los

³⁶Esto impacta hasta en la concepción misma de la legitimidad por activa del proceso, permitiéndose que participen cualquier interesado en garantizar el derecho fundamental, no exigiendo la calidad de afectado. Esta nueva tendencia se presenta para evitar la limitación de su disfrute a quienes no pueden defenderse procesalmente. (Ver. Pérez Luño, 2006:36-42)

países y van a cambiar las relaciones económicas y jurídicas. La sociedad comienza a inducir en el individuo la reducción de su “área privada” para poder recibir servicios eficientes: entregar datos de su estado de salud, informar de las condiciones de vida de sus hijos a las autoridades, informar acerca de su trabajo y sus ingresos al sistema de seguridad social. Al respecto menciona la profesora Matilde Zavala (1982:13):

“Hasta hace un tiempo relativamente reciente la intimidad no había sido sentida como un bien frágil y valioso. Ello solo ha ocurrido cuando la complejidad de la vida actual (...) han hecho peligrar la intangibilidad espiritual del hombre, y advertir el tremendo riesgo de alienación o dislocación que implicaría la carencia o mutilación de la intimidad”

La esfera privada de cada persona comienza a ser el atractivo principal de la comunidad que quiere conocer más y luego de las empresas o gobiernos para analizarlos con sus sistemas de información y ofrecer servicios más adecuados. Las personas se ven asediadas del apetito por su información personal o se ven con la presión social por que se rinda a preservar esa esfera privada. “Un tratamiento negligente, ilegal o no ético de la información sobre las personas puede traducirse en una violación de sus derechos y libertades (...)” afirma el profesor Nelson Remolina (2013:7) (ensentido similar Zabala, 1982:15)

Los teóricos del derecho comienzas a formular propuestas para regular el uso de las nuevas tecnologías de la información y la comunicación que se están utilizando para tratar masivamente los datos personales. En un primer momento adscriben el interés jurídico a la protección de la intimidad, que fue invadida a niveles preocupantes para quienes dieron el acceso a través de esas actividades masivas de tratamiento de la información, provocando una serie de afectaciones a los individuos con grandes consecuencias jurídicas. A continuación se tocará el impacto de las nuevas tecnologías en la noción jurídica de la intimidad, las actividades que configuraron este cambio y los potenciales problemas que pueden afectar la intimidad personal.

a) El Derecho fundamental a la intimidad ante la tecnología

El derecho a la intimidad pertenece a la primera generación de los derechos humanos, está vinculado profundamente al derecho a la personalidad³⁷ del ser humano, le permite proyectar la acción de su libertad en sociedad.

Se define entonces como un derecho a no ser molestado en el ámbito de la vida personal y familiar, como un derecho a estar solo (Warren & Brandeis, 1890:193). Tiene un surgimiento jurídico reciente, en el año de 1966 en Europa y en 1890 en los EE.UU. como *privacy*; la filosofía política ha reflexionado acerca de su importancia desde la revolución francesa. Se define en términos concretos como “(...) derecho de toda persona a mantener fuera del conocimiento de terceros aquellos aspectos de su vida corporal o anímica que le provocan recato o pudor, aun cuando no afecten su honor, imagen o integridad física o mental, toda vez que le resultan íntimos, no obstante la falsedad o veracidad objetiva de su contenido.” Es un derecho a mantener la reserva de la información personal y las intromisiones materiales o psicológicas sin permiso.

La intimidad o privacidad ha sido definida como una garantía de no ser molestado por ninguna clase de olores³⁸, de ruidos, perturbaciones en su hogar y luego se extendió hacia los aspectos más recónditos de la persona que se relacionaban un poco con los derechos de la reputación personal: el buen nombre, la honra y el honor, pues cuando estos valores eran respetados en un hombre y una mujer, ambos podían vivir tranquilo en sociedad³⁹. Los derechos de la reputación tienen consecuencias materiales y psicológicas claras: reducción de la autoestima, pérdida de ingresos por la baja reputación social; mientras que la lesión a la intimidad afectan los sentimientos de la persona, el aspecto espiritual, pues cuando las personas

³⁷Proviene de Persona que significa actor o intérprete. En sentido jurídico expresa la posición jurídica que le reconoce el ordenamiento jurídico al sujeto cuando se tienen determinados supuestos de hecho.

³⁸ Al respecto Samuel Warren y Louis Brandeis(1890:193) le llaman “the law of nuisance”

³⁹ So regard for human emotions soon extended the scope of personal immunity beyond the body of the individual. His reputation, the standing among his fellow-men, was considered, and the law of slander and libel arose. [Entonces en lo referente a las emociones humanas prontamente se extiende la protección física más allá de lo que estrictamente era el cuerpo]

no sienten un espacio que sea propio e impenetrable sin su permiso, sienten que están atrapadas por la sociedad y no pueden escapar de ella. Por otro lado se diferencian de los secretos industriales, en cuanto a que la información se conserva confidencial porque representa una ventaja económica que permite explotarse frente a otros negocios.

Los doctrinantes Samuel Warren y Louis Brandeis afirman que el primer ataque se dio con las empresas periodísticas, que han perturbado la tranquilidad de los hogares, de las personas de bien y comprometido el buen nombre de todos al querer buscar información y documentos que llamen la atención de los lectores. Al respecto afirman Warren y Brandeis (1890:195): “Por años se ha sentido que el derecho debe solucionar el problema de la circulación no autorizada de retratos sobre la vida privada de las personas y la malvada invasión de la privacidad por los periódicos, largamente sentida, ha sido recientemente discutida por un escritor capacitado”⁴⁰[Traducción del autor]. Concluyen que la intimidad es un derecho de la personalidad que da la garantía de que nadie puede obligar a publicar información o documentos referentes a una persona, en tanto que su ámbito de circulación quiere que sea restringido o nulo y además no se tenga un interés público grande en su figura.(Warren & Brandeis, 1890:205,214-215) Se aclara que está excluida la información que exprese algo de manera particular o diga aspectos negativos de la persona que se protegen por el derecho de autor y el derecho a la honra. Esta definición coincide con los elementos de la expuesta por la profesora Matilde Zavala (1982:87): un espacio ideal reservado, expresiones propias del individuo, desconocidas para la mayoría de las personas.

El derecho a la intimidad, de la mitad del siglo XX en adelante ve como una amenaza potencial las tecnologías automatizadas cuando comienzan a usarse de varias maneras en los tratamientos de datos personales (Remolina-Angarita, 1994, P.192)(Pérez Luño,2008:32) que acumulan información y generan una nueva clase de poder sobre las personas: el poder informático. (Ver en este sentido Puccinelli, 2004:473)

⁴⁰ For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons;and the evil of invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer. [Warren & Brandeis,1890:195]

Nuestras sociedades en los años 60 comienzan a llamarse sociedad de la información gracias a dos factores importantes: la potente capacidad de cómputo y el interés por aplicarla en el análisis de información para tomar decisiones vitales en empresas e instituciones públicas. Las implicaciones son profundas que pueden usarse o en el futuro existir medios para hacer identificable con una persona ciertos datos que estaban anónimos o se encontraban almacenados, con miras a obtener un provecho económico o social más efectivo.

Al final del siglo XX el poder informático aumenta su influencia a costa de la efectividad relativa de las facultades otorgadas a los sujetos (Remolina Angarita, 2013:2) motivado por conseguir el uso eficiente y analítico de la información. A principios de este siglo se designa esta amenaza potencial a la intimidad como un indebido tratamiento de información.

Cuando la información alcanza un valor tan alto, que es comparado al petróleo como fuente de riqueza, se acentúa el interés por garantizar que ese análisis o de la información se realice sin vulnerar derechos humanos. Se concibe que el adecuado tratamiento de la información personal debe reconocerse como derecho fundamental porque se necesita vincular las organizaciones tratantes o recolectoras de información personal a un cambio en las políticas de tratamiento de la información según los estándares y principios formulados alrededor del mundo puesto que el desconocimiento de las condiciones del procesamiento de datos le dificultan a la persona el control del uso de sus datos y la calidad de la información que se tiene de él.

En la medida que los modelos de negocio y entidades públicas comienzan a utilizar la información privada de las personas para ofrecer mejores servicios y productos comienza la preocupación acerca de la protección de datos. Internet ha acelerado los procesos en los que la información es el activo principal de muchas empresas. Por mencionar ejemplos la más conocida es Facebook, WhatsApp, Instagram, Snapchat y otras menos conocidas como Tumblr, Yik Yak o Square.

El Derecho reacciona al impacto de la computación que se está desarrollando y se propone el derecho a la autodeterminación informática o derecho al control de la información personal que está almacenada en las bases de datos para que las personas no queden tan expuestas en los aspectos importantes de su vida privada.

La doctrina norteamericana, con WESTIN⁴¹ y FRIED⁴² contribuyó mucho a revalorizar la privacidad de manera más activa, formulándola como la necesidad de saber que están haciendo con nuestros datos, para que nos lo pidan, como los utilizan. Se concibe como el *“right to control information about oneself”*. Esta faceta adicionada consiste en un nuevo derecho a ejercer una participación en el control de los datos personales almacenados, no simplemente conociendo lo que tienen de cada persona sino solicitando a través de mecanismos procesales que obliguen al debido tratamiento de esos datos (esto es de acuerdo a los principios estándar reconocidos internacionalmente), que consistirían en usarlos para los fines que fueron pedidos y autorizados por el titular del dato. En esta tercera faceta de la protección de datos personales se equilibra el poder informático y se completa el trípode de elementos que conforman la moderna concepción del derecho a intimidad: acceso consentido, conocimiento informativo y control del tratamiento.

Hay una nueva faceta surgiendo del derecho a la intimidad que no niega la intromisión en la vida privada de la sociedad y da una facultad jurídica a las personas para controlar el uso de los datos y evitar o evidenciar las violaciones producidas, que son de dos tipos (Remolina, 1994:198): i) acceso inadecuado o sin permiso a la información de la persona o a su esfera personal, con técnicas para obtener la información o con software o hardware de grabación de la voz o de la imagen o combinados; ii) Abuso del permiso otorgado, cuando la persona autoriza para un fin determinado pero se da cuenta de que se utilizó para otro no incluidos.

⁴¹*Privacy and Freedom*, publicado en 1967

⁴²*Privacy*, publicado en la Revista Yale Law Journal en 1968

b) Actividades que podrían afectar la intimidad de los individuos

La información se transforma en un activo importante para las organizaciones y las personas naturales⁴³, es poder para muchos fenómenos como el gobierno electrónico, el comercio electrónico, las redes sociales virtuales, la investigación biotecnológica, la investigación genética. El profesor Nelson Remolina Angarita (2013:4-5) refiere todo este proceso como big data, entendiendo que “(...) se basa en el uso de ingentes volúmenes de datos que son analizados y relacionados desde diferentes variables para sacar conclusiones, innovar, predecir, tomar decisiones (...) la idea del big data es sacar el máximo provecho de grandes volúmenes de información”, esta nueva tecnología representa un reto para el derecho, quien reacciona intentando regularla por los causes más provechosos para los dos intereses en juego: la dignidad humana y el principio de la libre empresa. De la coordinación en armonía de ambos intereses se podrá aprovechar en todo su esplendor uso potencial que abren las tecnologías para el big data.

Los servicios en que se apoya el big data son el cloud computing y la ingeniería del software, según el National Institute of Standards and Technology se define al primero como “un modelo para habilitar el acceso a un conjunto de servicios computacionales de manera conveniente y por demanda, que pueden ser rápidamente provisionados y liberados con un esfuerzo administrativo y una interacción con el proveedor del servicio mínimos”. (cit. por Remolina Angarita, 2013:6) y al segundo como un “(...) proceso, un conjunto de métodos y una serie de herramientas. (...) el establecimiento y uso de principios fundamentales de la ingeniería con objeto de desarrollar en forma económica software que sea confiable y que trabaje con eficiencia en máquinas reales.⁴⁴”

Las actividades posibles que se engloban como tratamiento indebido de datos personales son: i) *function creep* o uso incompatible con la finalidad inicial consentida ii) Recolección, almacenamiento y uso sin la autorización y iii) divulgación de información.

⁴³Debido a que se usan para analizar conductas, identificar patrones, crear perfiles virtuales de los usuarios de servicios.

⁴⁴Ver más en Pressman, Roger (2010). Ingeniería del software, un enfoque práctico. México: McGraw-Hill. Pág. 11

i) Uso incompatible con la finalidad inicial consentida se presenta cuando la información personal se utiliza para un propósito distinto del inicialmente informado y consentido. ii) La recolección, almacenamiento y uso sin la autorización se presenta cuando la persona desconoce que otra esté usando información personal que le concierne, en el ordenamiento jurídico colombiano existe un tipo penal que sanciona esta conducta, más adelante se detallarán los resultados del análisis. iii) La divulgación de información es publicar datos que se comparten con la persona. Al respecto el profesor Nelson Remolina (2013:13) afirma que es difícil garantizar un uso adecuado de nuestros datos, no debe sorprendernos que muchas veces se incumpla.

c) Los daños y lesiones causados por el indebido tratamiento de datos personales

Mediante las actividades masivas de tratamiento de la información mencionadas anteriormente se podrían estar afectando los derechos de la personalidad como el derecho a la imagen, el derecho a la honra, el derecho al buen nombre y el derecho a la dignidad humana. Estas conductas que afectan la persona son consideradas hechos ilícitos pues van contra el ordenamiento jurídico,⁴⁵ la responsabilidad civil se fundamenta en la existencia de hechos ilícitos cometidos que generan un impacto en los intereses protegidos de las personas. Al respecto dice Tamayo (2007:7):

“Como se ve, el hecho ilícito consiste siempre en el incumplimiento de obligaciones contractuales, cuasicontractuales, legales o simplemente en el incumplimiento del deber general de prudencia. De allí que podamos afirmar que la responsabilidad civil encuentra su fundamento jurídico en los hechos ilícitos (...)”

Cuando se cometen estos hechos ilícitos y generan una afectación a la persona surge la obligación de indemnizarle por los perjuicios causados. Pueden identificarse los tres elementos

⁴⁵ Toda conducta realizada por el hombre generará efectos jurídicos, bajo la teoría de los hechos jurídicos, algunos serán queridos y conformes a la ley (Tamayo, 2007:5), otros no como el incumplimiento de la obligación o realizados bajo negligencia o culpa, estos últimos son hechos ilícitos.

necesarios para adjudicar la responsabilidad de indemnizar a una persona que comete un hecho ilícito atentatorio de la intimidad: la conducta, el nexo causal y el resultado dañoso a otro (Alessandri, 1943:28). El interés protegido del derecho a la intimidad es perturbación de la intimidad, esto representa un daño moral, pero en ocasiones hace generar un el daño patrimonio económico de la persona.

La conducta que atenta contra la intimidad puede identificarse a partir del ingreso sin autorización al ámbito privado, esto puede hacerse mediante un real ingreso físico o a través de la divulgación de información por la confianza depositada o por accidente; el nexo causal será el vínculo que demuestra la dependencia de la producción del daño frente a la conducta realizada; el daño al otro causado en principio puede ser a la imagen de la persona, especialmente su reputación, daño moral o a la afectación de sus negocios o de los negocios de terceros (caso de ser presidente de una compañía cotizada en bolsa a quien le sacan fotos íntimas sobre sus gustos sexuales)⁴⁶. En muchas ocasiones es difícil recuperar este equilibrio o tranquilidad y se vuelve más pertinente una reparación monetaria que cualquier acción que pueda volver al punto inicial aspectos concernientes a su buen nombre u honor. Se tiene en cuenta el dolo o culpa para medir la intensidad del daño causado.

⁴⁶Sobre la indemnización de daño generado por la vulneración del derecho a la intimidad se produce al perturbarse ese sentimiento por otro de intranquilidad y zozobra.

Derecho de Protección del Dato Personal y el Habeas Data

“El dato se constituye entonces en el elemento Básico de información sobre eventos o cosas.”
Ernesto Lleras⁴⁷

En la sección anterior se han visto los orígenes filosóficos del derecho a la protección de datos personales en el principio general de la libertad, su afectación por las nuevas tecnologías de tratamiento de datos personales y la reacción de los ordenamientos jurídicos para mantener ese espacio personal libre de accesos no autorizados o de lo que se llama la polución de las libertades.

Ahora se entra a analizar como configuró el ordenamiento jurídico la reacción para proteger la información conectada con la privacidad. De antemano adelantamos la importancia que tiene la independencia actual de la Protección de Datos Personales como disciplina jurídica autónoma que se encarga de estudiar los aspectos jurídico- sustanciales y jurídico- procesales de la nueva tutela jurídica que se concede a esta área de la realidad. Esto lo podemos deducir cuando el Profesor Gonzalo Pérez Salazar la define, apoyándose en el profesor Oscar Pucinelli, como “(...) el conjunto de normas y principios que, destinados o no a tal fin, y con independencia de su fuente, son utilizados para la tutela de diversos derechos de las personas – individuales o jurídicas – que pudieran verse afectados por el tratamiento de datos nominativo (...) ese nuevo derecho incluye el de “autodeterminación informática”, “autodeterminación informativa”, “libertad informática”, information control y *habeas data*.”(Pérez, 2013:682)

En los estudios, que la doctrina ha realizado sobre el derecho de la protección del datopersonal, se encuentra que está representando sustancialmente por el derecho fundamental de la protección de datos personales y por la parte procesal por el Habeas Data. El profesor Hondius lo define “aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual de la intimidad del procesamiento manual o

⁴⁷Citado por la Corte Constitucional en Sentencia T-414 de 1992.

automático de datos” (Cit. por Puccinelli,2004:475). En su faceta procesal la disciplina del derecho de la protección del dato personal busca las herramientas jurídicas y técnicas más adecuadas para garantizar los derechos en cabeza de cada uno de las personas titulares de datos almacenados en bases computacionales, mecánicas o manuales.⁴⁸

La Sentencia 254 del 20 de julio de 1993, proferida por el Tribunal Constitucional español, es un ejemplo de la forma como se entiende el derecho a la protección de datos personales en su aspecto sustancial: es una garantía constitucional que incentiva una posición más activa de la persona con sus datos, otorgando derechos de control y revisión acerca del uso que se hace.⁴⁹En la actualidad, una vez asentado el reconocimiento de derecho fundamental, se continua con el énfasis en mecanismos de diversa naturaleza para garantizar que no se pierda el control de ese espacio personal al que han accedido, conocido y almacenado las personas naturales y jurídicas privadas o públicas.

La justificación para la tutela jurídica del tratamiento debido del dato personal es la conservación de la libertad sin obstrucciones y la ausencia de afectación a la dignidad humana⁵⁰, de esta manera la persona puede ejercer su autonomía conforme a su querer y no es determinada por las propuestas comerciales y estatales que le son ofrecidas. El reconocimiento de la afectación que puede tener la tecnología de base de datos en la dignidad humana se materializa en la elevación de la tutela jurídica del debido tratamiento de datos personas a derecho fundamental, con una estructura constitucional específica.

A partir de esta exposición se navegará por las aguas que analizan la incidencia de los anteriores argumentos en el reconocimiento de derecho fundamental al debido tratamiento del

⁴⁸Al respecto Pérez(2013:684) menciona la Resolución No. 0010-HD-2003 del Tribunal Constitucional Ecuatoriano(ahora corte constitucional)

⁴⁹Al respecto dicen en sus considerandos el Tribunal Español: “La llamada «libertad informática» es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data). (...) Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados (...) donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos (...) que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente p protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente(...)”

⁵⁰Al respecto las primeras sentencias del Tribunal Constitucional español, la 254 de 1993 y de la Corte Constitucional colombiana, la T-414 de 1992, lo corroboran.

dato personal, para determinar el interés del ordenamiento jurídico en garantizar su efectividad a través de mecanismos específicos de naturaleza constitucional, legal o administrativa.

La protección jurídica del dato personal

Antes de entrar a mirar como se ha desplegado la protección del ordenamiento jurídico hacia la persona y su información personal, se hace necesario adoptar una definición de dato personal, como bien jurídico protegido, para los efectos de este trabajo; acudiremos a los trabajos de reconocidos doctrinantes sobre el tema⁵¹, a los dictámenes emitidos por la autoridad europea encargada de cumplir la directiva de protección de datos personales, la definición encontrada en la jurisprudencia constitucional y la enunciada por el artículo 2° de la ley 1581 de 2012 que regula la protección de datos personales en Colombia.

a) Definición de dato personal según la norma europea

La Directiva 95/46/CE de la Comisión Europea define dato personal como “(...) *toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*”.

El Grupo del artículo 29 de la Comisión Europea analizó la definición en el dictamen 4 de junio 10 de 2007, donde concluyó“(...) una serie de orientaciones sobre cómo debe entenderse y aplicarse el concepto de datos personales (...)” (CE, 2007:27). El análisis respectivo se centra en lo que ellos consideran cuatro componentes principales del concepto: “toda información”⁵², “sobre”⁵³, “identificada o identificable”⁵⁴, “persona física”⁵⁵; estos

⁵¹Merece destacarse el cuadro comparativo de definiciones que elabora el profesor Nelson Remolina Angarita(2013:135) denominado “TABLA 8, Definición de dato personal en diversos documentos internacionales”, que hace recopilación de conceptos del dato personal expuestos por diversas organizaciones, coincidiendo más o menos en los elementos centrales que expone el modelo europeo.

⁵² “El término “toda información” comprende la que pueda decir algo de una persona o hacer que asociemos alguna idea o circunstancia con ella(Cfr.CE,2007: 6-9)

cuatro componentes hacen referencia al conjunto de afirmaciones, opiniones o comportamiento que expresan algo de una persona específica o que pueden darse indicios suficientes para distinguirlo, sin importar la veracidad de lo que representen o el ámbito de la actividad de la persona a que se refiera o el medio en el cual se almacena (físico, electrónico, mecánico).

Todo tratamiento de información que cumpla las características anteriormente mencionadas se considerará que se realiza sobre un dato personal y es posible que sea objeto de la aplicación de las normas de la directiva, cumpliendo con unos subsiguientes requisitos de aplicación que dependen de estar dentro o no de las excepciones al tipo de tratamiento realizado, del dato personal tratado y los posibles intereses legítimos del responsable del tratamiento de datos personales. Al respecto menciona la directiva que una “(...) mejor opción es no restringir indebidamente la interpretación de la definición de datos personales, sino tener en cuenta que existe una considerable flexibilidad en la aplicación de las normas a los datos. “(CE, 2007:4)

b) Análisis de la Definición aceptada en el ordenamiento jurídico según la jurisprudencia constitucional

El literal c del artículo 3 de la Ley Estatutaria de Protección de Datos Personales (LEDP) define el dato personal como:

Art. 3. Definiciones

(...)

“c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”

⁵³ El término “sobre” indica que trata de una persona cuando el “dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa”, son tres criterios alternativos que indican cuando la información se refiere a una persona: **contenido, finalidad y resultado** (CE,2007:10)

⁵⁴“Identificada o identificable” hace referencia a que la información puede indicar que pertenece a una persona, esto se puede deducir a través de los criterios mencionados puede efectivamente habilitarnos para distinguirlo de otro que tenga rasgos semejantes o ejecute una actividad similar, por cualquier medio directo o indirecto.

⁵⁵Todo ser humano que tiene el rasgo de ser vivo y existente.

Esta definición es resultado de sintetizar en un enunciado las características del dato personal, que la Corte Constitucional analizó a lo largo de su jurisprudencia; la sentencia T-414 de 1992 menciona que son tres las características: “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.” Estos elementos que lo caracterizan son corroborados en sentencia C-748 de 2011 con ocasión del control de constitucionalidad al proyecto de ley que se convertiría en la Ley Estatutaria de Protección de Datos Personales (LEPDP)

La definición legal de dato personal que realiza el legislador colombiano en la ley 1581 de 2012 hace palpable la influencia de la directiva 95/46/CE y adecuadamente aplicable el análisis estructural del concepto de dato personal realizado por el grupo de trabajo. En esto se encuentra de acuerdo la Corte Constitucional colombiana cuando hace el análisis de constitucionalidad mediante la sentencia C-748 de 2011. En efecto puede apreciarse que tiene los mismos cuatro elementos estructurales: “Cualquier información”, “vinculada o que pueda asociarse”, “una o varias personas naturales”, “determinadas o determinables”.

En el caso colombiano, “cualquier información” lo define la Corte Constitucional al decir que se limita a los aspectos que se encuentren en el ámbito privado de la persona o a aspectos que no es tan difícil acceder, “vinculada o que pueda asociarse” implica que de la información puedan conocerse aspectos del ámbito privado de la persona como su personalidad, sus hábitos de compra, sus actividades preferidas. Cuando se habla de “una o varias personas naturales” debemos remitirnos a la definición de “persona natural” como todo individuo de la especie humana que haya nacido y sobrevivido un instante siquiera y que se enmarca por los artículos 74⁵⁶ y 90⁵⁷ del código civil colombiano. Adicionalmente la Corte

⁵⁶ ARTICULO 74. PERSONAS NATURALES. Son personas todos los individuos de la especie humana, cualquiera que sea su edad, sexo, estirpe o condición

Constitucional extiende la tutela jurídica a las personas jurídicas, en tanto administran datos personales, bien sea de sus empleados o de sus clientes o usuarios:

“Ciertamente, la garantía del habeas data a las personas jurídicas no es una protección autónoma a dichos entes, sino una protección que surge en virtud de las personas naturales que las conforman. Por tanto, a juicio de la Sala, es legítima la referencia a las personas naturales, lo que no obsta para que, eventualmente, la protección se extienda a las personas jurídicas cuando se afecten los derechos de las personas que la conforman.” (Sentencia C-748 de 2011, subrayado y cursivas fuera de texto)

El dato personal es definido a partir de lo anterior como el conjunto de información característica⁵⁸ que pertenece a una persona física o jurídica y que al juntarse en un lugar, llamada base de datos, permite determinar fácilmente la identidad de la persona. El profesor Nelson Remolina (2013:133) lo define simplemente como cualquier aspecto que hace alusión sobre una persona.

c) Clasificación del dato Personal

Analizada la definición de dato personal se encuentra que dentro de ella caben muchas clases de información: comercial, financiera, de buena imagen, de salud, penal, educativa, familiar, intelectual, religiosa, racial; la clasificación según el contenido del dato se debe a que la persona tiene un margen de actuación bastante amplio, en ejercicio de su potestad y de las relaciones sociales o jurídicas que entable, pues estamos en una sociedad.

⁵⁷ ARTICULO 90. EXISTENCIA LEGAL DE LAS PERSONAS. La existencia legal de toda persona principia al nacer, esto es, al separarse completamente de su madre. La criatura que muere en el vientre materno, o que perece antes de estar completamente separada de su madre, o que no haya sobrevivido a la separación un momento siquiera, se reputará no haber existido jamás.

⁵⁸Esos rasgos físicos, psicológicos, culturales o intelectuales; ahora en el sentido moderno también el conjunto de acciones que expresan preferencias sociales, por ejemplo cuando hacemos check-in de localización en un lugar que se encuentra en determinado sector, junto a otro grupo de personas, se puede deducir ciertos parámetros básicos de nuestra identidad: cuanto gastamos, cuales son nuestros sitios que más frecuentamos, con quienes, que aspectos influyen en nosotros.

Sin embargo para el ordenamiento jurídico es reconocido con mayor importancia la clasificación realizada a partir del grado de intensidad en la aplicación de los principios de administración o tratamiento de datos personales y de la ley estatutaria que se define por la accesibilidad y sensibilidad de la información. Esta clasificación es de cinco tipos de datos personales: pública, semi-privada, privada, sensibles y excluidos del tratamiento.

El grado de intensidad en la aplicación se determina pues por la accesibilidad y sensibilidad. Sobre la accesibilidad, es un criterio formulado a partir del permiso de acceso y recolección del dato. Con respecto a la sensibilidad y , siguiendo al profesor Nelson Remolina (2013:136 y ss.) a partir de lo que él llama “sensibilidad de un dato”, se define como una cualidad adjudicable a un dato que puede representar un riesgo potencial por el mismo contenido o por el uso contextual en que se realice, frente al primero se tienen por ejemplo los datos genéticos o referentes a su salud de una persona y frente al segundo los datos personales sobre filiación política y religiosa en un país que se encuentre en guerra o que sea una dictadura.

A partir del tipo de dato personal identificado deberán aplicársele los parámetros que se haya definido en leyes especiales y en la ley general, así como también podrá evaluarse en un proceso administrativo sancionatorio o judicial la gravedad que produce la inobservancia de las normas en lo referente al daño por el tipo de dato personal y la posible comisión de un delito. Ciertamente por última razón puede afirmarse que en cuanto a tratamiento de datos personales, el régimen de responsabilidad civil es de naturaleza objetiva, en la sección de las herramientas jurídicas se ampliará un poco esta idea.

Para concluir: aplicar el criterio de accesibilidad permite identificar quien es el legitimado para hacer el tratamiento de los datos y quien el responsable; el criterio de sensibilidad hace posible comprender como debe realizarse el tratamiento, es decir, que aspectos de la LEPDP se aplican frente a otros. Estos dos criterios son una buena fuente de decisión sobre calificar un tratamiento como indebido o ilícito.

i) Dato Personal Público: Se define por exclusión, según el artículo 3° del Decreto 1377 de 2013 en su numeral 2° es aquel dato que no es semiprivado, privado o sensible. A renglón seguido describe algunos posibles ejemplos como registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Esta definición tiene el riesgo, en opinión del profesor Nelson Remolina (2013:140), que por su estructura en blanco y supeditada a lo que se definan en las otras clases de datos, de volver públicos muchos datos personales protegidos, al ser información pública, por esto no requerirá del consentimiento del titular. Este riesgo es palpable cuando la Corte afirma que los datos públicos o “información pública, en tanto no está relacionada con el ámbito de protección del derecho a la intimidad, recae dentro del ejercicio amplio del derecho a recibir información (art.20 C.P.) y, en consecuencia, es de libre acceso” (Sentencia C-1011 de 2008)

La razón por la cual frente a estos datos personales no se requiere el consentimiento es que la finalidad de la publicidad ha sido consentida por el titular del dato personal. Por esta razón se diferencia de la información que esta “disponible” en internet, que es dada al mundo sin la autorización.

ii) Dato semi-privado: Lo define la ley 1266 de 2008 como aquel dato que “no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento puede interesar no sólo al titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero o crediticio (...)”. El criterio que impera es el interés pertinente de acceso legítimo que se tenga. Si se requiere autorización previa en tanto comporta aspectos privados que entran a conocimiento de un grupo de personas por razón de una relación, generalmente jurídica o comercial.

iii) Dato personal privado: Aquel dato personal que es exclusivamente relevante para el titular, dado que le pertenece a su naturaleza íntima o reservada; sólo se obtiene mediante orden judicial en cumplimiento de sus funciones. Así se deduce de la lectura del literal h) artículo 3° ley 1266 de 2008 y del literal f) del artículo 4° de la ley 1581.

El profesor Nelson Remolina (2013:142-144) pone de ejemplo los libros de los comerciantes, las historias clínicas, la información tributaria, información que reposa en la Registraduría, etc., y podrían agregarse los informes de inspección judicial a una vivienda que describen⁵⁹ por dentro sus elementos.

Este es el caso paradigmático de los directorios telefónicos que deben cumplir los requerimientos de protección de datos personales, según la Resolución 3066 de 2011 de la Comisión de Regulación de Comunicaciones. Esto significa que pese a su acceso público, estos datos de los directorios deben cumplir con los principios de protección, entre esos el de autorización y finalidad tanto del responsable (empresa de telecomunicaciones) como del usuario(a quienes se les envía el directorio). Por esta razón “el titular del dato puede en cualquier momento solicitar que se excluya su información del directorio telefónico o que dejen de llamarlo (...)” (Remolina, 2013:149)

iv) Dato personal sensible: Es aquel dato que al ser tratado sin unos parámetros estrictos puede comprometer derechos o libertades de la persona. Un ejemplo de esta clase de datos son los datos genéticos, biométricos⁶⁰, los datos sobre pacientes con VIH, los datos del Registro único de víctimas. Así los definió la LEDPD:

“Artículo 5°. Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva 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.”

⁵⁹Claro que en el marco de un proceso es que se obtienen y ofrecen. Fuera de este ámbito esta prohibido hacerlo sin el consentimiento.

⁶⁰Estos datos determinan características físicas y psicológicas de la persona.

Se permite su tratamiento cuando se dé el consentimiento del titular, se requiera para proteger la integridad personal del titular del dato personal y no este en capacidad de autorizar o en desarrollo de actividades legítimas por una Organización No Gubernamental o fundación, sea necesario para ejercer un derecho en un proceso judicial y cuando se utilice con fines históricos, científicos o estadísticos.

Al respecto la Corte Constitucional en sentencia C-1011 de 2011 acotó sobre el dato sensible lo siguiente:

“(…) 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.”

v) Datos excluidos del tratamiento: Este caso particular colombiano se encuentra en el artículo 7 de la LEPDP que prohíbe el tratamiento de datos personales de niños, niñas y adolescentes, permitiéndolo cuando el dato es de naturaleza pública. Sin embargo a nivel internacional se tienen borradores de normas que establecen el permiso, incluyéndolo dentro de los datos sensibles bajo el requisito del consentimiento del padre de familia o del menor que tenga capacidad relativa.

d) Protección jurídica reconocida

La protección jurídica comienza con el desarrollo conceptual de la libertad informática en la Ley de protección de datos personales del Land de Hesse del 7 de octubre de 1970, luego en 1973 la ley sueca, en 1974 la Privacy Act de USA. A nivel constitucional se incluye en

Portugal (art.35 en 1977), España (art.18 en 1978). Esa “libertad informática” era en realidad muy restringida pues se limitaba a dos de los actuales derechos ARCO: acceso y cancelación.

La tutela jurídica inicia nivel Iberoamericano a partir de los años 1970 con España y Portugal, siendo la Constitución de este país un poco más rica en descripciones y contemplando en su totalidad la actividad relacionada con su recolección, almacenamiento y análisis de acuerdo a unos parámetros técnicos y jurídicos que al dato aislado como tal; las afectaciones que ponen en desventaja frente a sus semejantes en las decisiones que toma o verse desmejorado en sus condiciones por las decisiones que se tomen a partir del tratamiento del dato personal; la vulneración de derechos como la honra, la imagen, el buen nombre, la libre expresión, la libertad de cultos y asociación sindical y a nivel general con el principio de la dignidad humana. (Ver Puccinelli,2004:476)

Las consecuencias jurídicas que pueden generarse a partir de un indebido tratamiento de datos personales son nefastas al titular del dato. La situación se ha vuelto más explícita con el abaratamiento de tecnologías. Estos dos factores en conjunto han hecho volver el foco sobre las actividades de procesamiento para darle un escudo jurídico constitucional, lo que la hace suficientemente fuerte e importante para la agenda del estado social de derecho. La clase de protección jurídica que se otorga al dato personal (aunque como dice Puccinelli [2004:474] en sentido estricto se protegen son los” [...] derechos que puedan ser lesionados a partir de su desprotección [...]) es de elevado nivel, al reconocérsele la naturaleza de derecho fundamental.

El tratamiento adecuado de la información personal debe reconocerse como derecho fundamental por cuatro razones según Saarenpää (2003): “las exigencias de la democracia, la sociedad red, la búsqueda de la eficiencia y el complejo curso vital de la información”. Este nuevo derecho surge para vincular las organizaciones tratantes o recolectoras de información personal a un cambio en las políticas de tratamiento de la información según los estándares y principios formulados alrededor del mundo. Las condiciones del procesamiento de datos le dificultan a la persona el control del uso de sus datos y la calidad de la información.

Las Constituciones latinoamericanas que han reconocido el derecho a la protección de datos personales dan amplias facultades a las personas, que pueden ejercer en cualquier momento, generalmente le encomienda el desarrollo del procedimiento a la ley. Algunas constituciones desarrollan un procedimiento especial al que denominan Habeas Data (es el caso del artículo 200-3⁶¹ en la Constitución peruana de 1993 o el artículo 43 de la Constitución de Argentina) y otras lo asemejan al recurso de amparo o acción de tutela colombiana, como el caso de la Constitución de Paraguay de 1992 en su artículo 135⁶². Esta acción procesal “supondría algo así como *traer la información, o conversar los datos*” (Cursivas fuera de texto, ver. Eguiguren, 1997:120)

Por lo anterior algunos doctrinantes han encontrado que el derecho de la protección de datos personales se conciba como garantía, como acción procesal, como recurso dentro de un proceso judicial o una actuación administrativa o como derecho fundamental. Antes de entrar a mirar la clasificación del Habeas Data es necesario analizar los antecedentes históricos de América Latina para comprender mejor los argumentos propuestos acerca de la posible naturaleza jurídica de este derecho.

Antecedentes históricos en América Latina

El desarrollo histórico del derecho de protección de datos personales ha tenido una influencia notable de los países europeos y de Estados Unidos. Esta sección no se centrará en dar un recuento histórico del desarrollo legal de estos dos modelos de manera breve y sucinta, sino en los desarrollos legales históricos que han ocurrido en algunos países de América Latina. Los aspectos descriptivos de los dos modelos estándar se realizarán en la tercera parte del capítulo relativa al análisis del nivel de protección de datos personales de Colombia. En América

⁶¹“ Son garantías constitucionales (...) 3) La acción de habeas data, que procede contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, inciso 5° y 6° de la Constitución”

⁶²Podrá solicitar ante el magistrado competente la actualización, rectificación o la destrucción de aquellos, si fueren erróneos o afectaran ilegítimamente sus derechos”

Latina el profesor Oscar Puccinelli (2004:477) afirma que este derecho se ha desarrollado a nivel constitucional y legal.

El primer país que fija una regulación específica sobre el tema fue Guatemala en 1985, el enunciado normativo de la misma concentra sus esfuerzos en garantizar el acceso de los datos de personas almacenados por el estado y prohibiendo unas bases con lo que modernamente se considerarán datos sensibles: filiación política, creencias religiosas, padrones electorales⁶³; los desarrollos legales han desembocado en leyes sectoriales que tratan el procesamiento de datos dentro de las muchas temáticas: derecho del consumidor; o el acceso a la información pública.

Posteriormente Nicaragua en 1987 lo incorpora dentro del derecho fundamental a la intimidad, conservando el mismo patrón de tutela jurídica del anterior país. En el año 2012 expide una ley general sobre protección de datos personales muy completa porque establece los requisitos necesarios para permitirse la obtención legítima de datos personales, las obligaciones que corren por cuenta del responsable del tratamiento, una novedad interesante es la tipología de dato personal que fija (art.8°): informático, sensible, comercial y de salud; otra es la acción de protección de datos personales(art.48-50) de naturaleza administrativa porque judicial tienen el recurso de amparo (art.52); las infracciones bajo el principio de culpabilidad al tipificarlas en leves y graves.

Brasil en 1988 inicia una tendencia diferente, producto de circunstancias históricas como la salida reciente de una dictadura que aprovecho el tratamiento mecánico de datos de las personas para cometer torturas persecuciones (Puccinelli,2004:479-480), con la creación una garantía específica para protegerse de los peligros que causa la informática, esta herramienta le denomina Habeas Data, que significa poseer o controlar el dato, este pequeño cambio inicia la tendencia hacia una mayor regulación y dotación de herramientas a las personas dado el carácter judicial que se le otorga. El Habeas Data brasileño permite conocer y rectificar los

⁶³“Art. 31. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos”.

datos personales guardados en las entidades públicas⁶⁴. La regulación legal vino después y se enfocó en el mecanismo procesal así como en regular los bancos públicos de datos con leyes de diversos temas en 1990.

En 1991 Colombia lo regula en su Constitución introduciendo a las entidades privadas dentro de las obligadas para conocer, actualizar o rectificar los datos recogidos. El punto a resaltar principal es que en el tratamiento de datos personales se debe respetar no solo los anteriores derechos sino el derecho a la libertad y otros derechos que puedan vulnerarse.⁶⁵ El mecanismo de defensa preferido ha sido la acción de tutela y luego con su regulación legal a través de la ley 1581 de 2012 se establecieron la consulta, el reclamo y la queja. Aunque extraestatutariamente existen los tipos penales de la ley 1273 de 2009, el procedimiento administrativo sancionatorio y la responsabilidad civil por indebido tratamiento de datos que se deduce de las normas vigentes del código civil.

La Constitución paraguaya de 1992 le asigna la característica de acción procesal por la cual podrá “ante el magistrado competente la actualización, rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos”, es una novedad la consagración de una acción procesal de Habeas Data, como los brasileños, quizá debido a que hicieron parte de las dictaduras del Cono Sur que realizaron la *Operación Cóndor*. Luego se reglamentó solo los bancos de datos personales privados con la ley 1682 de 2001 reconociendo los derechos a la actualización (art.7°), de acceso (art.8°) el consentimiento informado (art.5°); esta ley se enfoca principalmente en las obligaciones comerciales y crediticias, no tiene el carácter de general. Posteriormente la reforman en el 2002 con la ley 1969 ampliando dando un papel más activo a la misma al declarar que regulara varias actividades realizadas en el procesamiento de datos personales (recolección, almacenamiento,

⁶⁴Art. 5. Todos son iguales ante la ley, sin distinción de cualquier naturaleza. Se garantiza a los brasileños y a los extranjeros residentes en el país la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad, en los términos siguientes:[...]LXXII. Se concederá *Habeas data*:

“a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; “b) para rectificar datos, cuando no se prefiriera hacerlo por procedimiento secreto, judicial o administrativo”

⁶⁵“Art. 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 bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de los datos se respetarán la libertad y demás garantías consagradas en la Constitución”.

análisis, distribución, la ley trae una novedad al consagrar excepciones; la novedad es la regulación del derecho de rectificación que está en la Constitución del país pero ausente en la anterior ley 1682.

La Constitución peruana de 1993 regula de manera integral el problema del acceso y el control de los datos personales con la acción de Habeas Data (Art.200, núm. 3º) y su separación del derecho a la protección de datos personales(art. 2º, núm. 5). El Habeas Data peruano permite ejercer el derecho de acceso a la información pública y a la tutela jurídica de los derechos reconocidos por la ley 29733 de 2011, se excluye de esta ley al regularse en el Código Procesal Constitucional del país; “(...) es una suerte de amparo especializado para la protección de ciertos derechos (...)” (Eguiguren, 1997:124). En el desarrollo legal se tiene la novedad de reconocer un derecho a ser indemnizado por los daños causados al titular o a los encargados (art, 27º ley 29733), sin embargo algunos doctrinantes critican que haga falta una regulación constitucional más incluyente de otros derechos, por ejemplo echa en falta que no puedan ejercerse los derechos de acceso y conocimiento a los datos almacenados en bancos privados o su rectificación (Eguiguren, 1997:128-130)⁶⁶

En 1994 se incorpora el Habeas Data en la Constitución argentina por medio de una reforma, estableciéndolo como una acción similar al recurso de amparo argentino en el inciso tercero del artículo 43⁶⁷. Posteriormente se expide la ley 25.326 para regular “la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos (...)”, está ley sigue los consejos establecidos por el modelo estándar europeo de protección de datos personales; merece destacarse que hace una descripción clara de los principios que regula el tratamiento de datos personales, la prohibición de obligar a que se proporcionen datos personales sensibles bajo cualquier supuesto (aunque

⁶⁶Para profundizar más ver Eguiguren, F. (1997), 5. EL HÁBEAS DATA Y SU DESARROLLO EN EL PERÚ *Ius et Praxis* vol. 3, N°1; ISSN 0717-2877. Recuperado el 18 de abril de 2016 en: <<http://www.redalyc.org/articulo.oa?id=19730111>>

⁶⁷ Artículo 43.- Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva. (...) Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en (continuación nota 66) caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.

se da permiso a la recolección y tratamiento cuando así lo exprese la ley, lo cual es un poco ambiguo), una regulación detallada de los supuestos de hecho permitidos de transferencia internacional de datos y la tipología de archivos que maneja(arts. 26-28). La normativa legal argentina tiene una regulación completa e integral del tratamiento de datos personales, de tal manera que cubre la mayor de la protección, de ahí que la Unión Europea le haya calificado con un nivel de protección adecuado para tratar datos personales de ciudadanos europeos.

Ecuador en su Constitución en 2008(Art. 66-19) denomina como como un derecho a la protección de datos personales y una correspondiente acción de habeas data (Art.49 de la Ley orgánica de garantías jurisdiccionales y control constitucional) para obtener todos los denominados derechos ARCARS⁶⁸: Autorizar, Revocar, Conocer, Actuaizar, Rectificar y Suprimir (eliminación).⁶⁹

En la Constitución de Venezuela, expedida en 1999, se regula como una acción independiente llamada habeas data a cargo del Defensor del pueblo (art.281) que protege los derechos ARCARS enunciados en el artículo 28 de la misma, para los casos de vulneraciones individuales se tiene la acción de amparo constitucional. No se encuentra expedida una normativa general que agrupe los aspectos procesales y sustanciales del derecho de la protección de datos personales.

En Bolivia el Habeas Data es de carácter correctivo, se llama acción de protección de la privacidad (Art. 130 de su Constitución) y se tramita según el procedimiento de la acción de amparo (Art.131-I). Por otro lado, los derechos ARCARS han sido regulados por medio de

⁶⁸Si bien esta clasificación la propone el profesor Nelson Remolina Angarita para identificar los derechos reconocidos en el ordenamiento jurídico colombiano es igualmente aplicable al caso ecuatoriano dadas las similitudes en los derechos reconocidos en todo el artículo 92 de su constitución.

⁶⁹ Artículo 92.Toda persona (...) tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma(...) consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados”.

decreto presidencial N° 1793 de 2013 en el artículo 56 en desarrollo de los derechos de los usuarios fijados en el artículo 54-6

Costa Rica en su Constitución no desarrolla el derecho a la protección de datos personales y lo incorpora dentro del derecho a la intimidad personal. Sin embargo expide la ley 8968 de 2011, que regula especialmente el fenómeno y se destaca por expresar la autodeterminación informativa (Art.4°) como principio ligado al deber de un legítimo y adecuado tratamiento del dato y derecho fundamental para controlar el flujo de información personal.

En Chile su constitución lo integra dentro del derecho a la intimidad, luego cuando expide la ley de protección a la vida privada (ley 19.628 de 1998) que regula con gran detalle todo el derecho de protección de datos personales que se halle en bancos de datos públicos y privados en su faceta sustancial y procesal, destacando esto último que regula un procedimiento para atender la falta de atención a los requerimientos del titular del dato hacia el responsable para respetar los derechos(Art.16) y una acción específica para reclamar el daño moral y patrimonial generado por el tratamiento de datos indebido(Art.23). La ley chilena (art.18) tiene en cuenta circunstancias bajo las cuales no se comunican los datos de morosidad como el estado de cesantía en el trabajo, debido a que potencialmente puede amenazar su buen nombre e imagen

El ordenamiento jurídico mexicano ha establecido la protección de los datos personales en el artículo 16 de su Constitución, desarrollándolo a través de la Ley Federal de Protección de Datos Personales que sigue una estructura similar a las anteriores normativas legales mencionadas.

En el análisis de las normas sobre Habeas Data en Latinoamérica casi todas siguen una estructura muy uniforme con unos principios, derechos de los titulares, obligaciones de los encargados y de los responsables del tratamiento de datos personales, un procedimiento de para hacer efectivo los derechos de los titulares (que varía en su naturaleza administrativa o judicial). Algunas detallan más en las facultades de la Autoridad de Protección y

cumplimiento de las normas, otras en los tipos de datos (Argentina), algunas en un procedimiento bastante detallado (Chile).

El Habeas Data en esta región del mundo tiene el espíritu de mantener alejados los intentos de “encarcelar” partes de nuestra alma, buscando repeler las injerencias no consentidas o las perturbaciones en el almacenamiento, registro y utilización. Pero no pueden olvidarse su carácter instrumental para obtener la efectividad del derecho al debido tratamiento de datos personales y otros derechos conexos fundamentales que pueden verse afectados y por ello es en sentido preocupante que en algunos países de los reseñados no contemplen mecanismos específicos más allá del procedimiento administrativo sancionatorio o de la acción de amparo constitucional. Garantizar el ejercicio de la libertad informática es la mayor consigna del Habeas Data.

Interpretaciones de su naturaleza jurídica en América Latina

En los ordenamientos jurídicos de varios países latinoamericanos se le da al derecho de la protección de datos personales la calificación de instrumental, emparentándolo junto al derecho de Habeas Data. Este derecho instrumental está en circunstancias también oscuras respecto a su naturaleza jurídica, siendo calificado como recurso, proceso, garantía, derecho autónomo (generalmente cuando se le mezcla con el derecho de protección de datos personales)

Algunos autores tienden a unir el procedimiento y el derecho fundamental en uno solo (Pérez,2013:586) , llamándole Habeas Data, dando claro predominio al carácter instrumental del derecho fundamental que surge, por ejemplo la profesora Isabel Palomino lo define como “un derecho fundamental de la persona de controlar y disponer sobre las informaciones a él referentes de carácter personal” (cit. por Pérez,2013:687) otros autores coinciden en lo esencial con la anterior definición como derecho fundamental del control de la información. Otros autores le dan preeminencia al aspecto sustancial, concibiéndola como una garantía constitucional al servicio de la tutela de los derechos fundamentales, se destaca la Corte

Constitucional colombiana en sentencia C-1011 de 16 de Octubre de 2008 quien la concibe como “(...) facultad al titular de datos personales de exigir de las administradores de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización o certificación de esos datos (...) de conformidad con los principios que regulan el proceso de administración de datos personales (...)”.

Se está de acuerdo con la definición de Habeas Data que formula Gustavo Marín García (Cit. por Pérez, 2013:689) como “ (...)mecanismo especial que sólo puede ser utilizado cuando se pretenda acceder, conocer el uso o la finalidad, la destrucción, actualización o rectificación de los datos o información que haya sido almacenada, sin o con el consentimiento del titular, en registros públicos o privados” porque concibe el instrumento al servicio del aspecto sustancial, separándolo tajantemente de este. Y es que el Habeas Data además de garantizar los derechos al debido tratamiento de datos personales, agrupados en los ARCO o ARCARS, tiene el fin de garantizar derechos sustanciales como el del honor, la intimidad, el buen nombre o la imagen.

El reconocimiento de derechos fundamentales y derechos humanos en la Constitución

El profundo interés por obtener espacios reservados a la intervención del Estado motivó las reflexiones filosóficas acerca de la existencia de una esencia común a todo ser humano, que podía comprenderse a través de la razón y la introspección. Fue un legado profundo de universalismo y racionalidad que nos llegó desde los estoicos en la antigüedad y que fue visto en la primera parte de este capítulo.

Sin embargo, cuando fueron ocurriendo los levantamientos revolucionarios de Francia y la independencia de las colonias americanas, se pensó que el Estado no podía estar del todo apartado y que era necesario para garantizar – que ironía tan grande – el respeto profundo de los derechos fundamentales al mismo tiempo que se le imponían ciertos límites en su actuación. Ciertamente la duda fue como evitar los anteriores momentos de absolutismo y control de la sociedad por un solo individuo o grupo pequeño.

La solución fue reconocer que el Estado era un sujeto de derechos y obligaciones y que debía estar vinculado a la ley, pero esta ley debía ser superior a las que profería (Pérez Luño, 2005:67). El origen de esta ley debía garantizar la suficiente legitimidad para que fuese también reconocida por la sociedad, la manera de conseguirlo fue dándole la soberanía para que se volviera el poder constituyente del Estado. Esa ley superior fue la Constitución, texto compuesto y normativo sobre asuntos tan dispares como la organización del estado, los principios que inspiran su actuación y los derechos fundamentales que protegen a todos sus ciudadanos.

La función inicial de los derechos humanos fue hacer de contención a la autoridad estatal, ahora hay un cambio de una concepción negativa de los derechos humanos a una concepción activa y participativa para su efectividad, radicada en cada una de las personas que ejercen los mecanismos. Es por esta razón que principalmente los derechos humanos fueron positivizados en distintos niveles⁷⁰, uno de ellos ocurrió cuando fueron incluidos en Constituciones y se les convirtió en derechos fundamentales; sin embargo cabe aclarar que no todos los derechos fundamentales pueden ser considerados derechos humanos.⁷¹

En esta sección nos enfocaremos en el proceso de reconocimiento de los derechos fundamentales en el ordenamiento jurídico, concluyendo en la importancia del estado constitucional y democrático de derecho como el principio de organización que impulsa todas las instituciones hacia el respeto de ellos. Para ello se adoptará la concepción estructural de las normas de derechos fundamentales que propone el profesor Robert Alexy.

⁷⁰Al respecto el profesor Pérez Luño(2005:67) habla de una *lex generalis*, esto es, principios generales reconocidos como la libertad, la igualdad, la solidaridad, la dignidad humana y una *leges speciales*, donde se desglosan los anteriores principios en aspectos más concretos vinculados con partes de la realidad humana.

⁷¹ Al respecto concluye el profesor Carlos Bernal Pulido en su estudio introductorio al libro de Robert Alexy(2007:LI) sobre la teoría de los derechos fundamentales: "Es innegable que los derechos fundamentales representan una institucionalización en el sistema jurídico de los valores de la teleología o de los principios que aparecen en la moral en forma de derechos humanos"

a. *Una aclaración preliminar: los Derechos fundamentales como derechos humanos positivizados*

Los derechos humanos son el desarrollo de los límites de la libertad de las personas cuando se convive en comunidad, como se explicó previamente en el capítulo sobre la concepción generacional de ellos. Es así porque permiten encauzar los límites de la acción humana, de ese estado de naturaleza que recuerda Locke (2006:19), dentro de la convivencia social en la cual nos desenvolvemos.

Los derechos humanos son un reconocimiento a la capacidad humana de elegir y de realizar todas las acciones que considere prudentes para el desarrollo de su preservación, con el propósito de asegurar el disfrute de las propiedades principalmente, de manera pacífica y segura.

Ahora como es difícil que todos los hombres puedan cumplir la ley en estado de naturaleza y en forma adecuada, se hace indispensable acuerdos en común que den unas normas básicas y la entrega del cumplimiento de las mismas a un tercero. Así lo afirma Locke (2006:126): “Y si no fuera por la corrupción y la maldad de hombres degenerados, no habría necesidad de que los hombres se separasen de esta grande y natural comunidad para reunirse, mediante acuerdos declarados, en asociaciones pequeñas y apartadas unas de la otras”. Estas asociaciones pequeñas en algún punto de la historia se unirán para formar grandes comunidades regidas bajo una sola autoridad gobernante: Estado.

El fin del Estado es organizar la comunidad según las orientaciones de la ley de la naturaleza, para que no se oponga a los derechos de los individuos. ¿Cuáles el criterio por los cuales el gobierno cumple la ley natural? Este criterio es el respeto a los derechos humanos, porque reconocen que existen valores intrínsecos a la naturaleza humana. Se menciona partes de lo que comenta el profesor Antonio Pérez Luño sobre la conversión en normas de los principios de derecho natural, pensados por los filósofos a raíz del cambio histórico devenido con el siglo de las luces, entre esos el de la libertad: “La nueva expresión [derechos del hombre] al igual la de “derechos fundamentales”, forjada también en este período [mitad del

siglo XVIII], revela la aspiración del iusnaturalismo iluminista por constitucionalizar, o sea, por convertirse en derecho positivo, en preceptos del máximo rango normativo, los derechos naturales”(Perez,2004:33) (corchetes fuera de texto)

Ahora bien como es necesario que estén reconocidos en la legislación del Estado para hacer una protección más efectiva, desde el punto de vista jurídico, se les incluye con enunciados normativos vinculantes. El lugar donde se incorporan estos enunciados es en la Constitución (Alexy, 2000:36,) específicamente en una sección que agrupa“los derechos fundamentales”, por ser la norma suprema del ordenamiento jurídico de cualquier país. Los derechos fundamentales tienen su origen en el mismo principio de la libertad, que debe protegerse frente a interferencias estatales y privadas.

b. Normas de derecho fundamental

La concretización de los derechos fundamentales se realizó a través de la formulación como derechos subjetivos en la Constitución, es decir derechos positivizados. La necesidad histórica de dar certeza jurídica a estos derechos, inicia el proceso de concretización bajo unos parámetros formales que terminaría en la adopción de la teoría de los derechos subjetivos como parte del derecho público para garantizar su protección estatal. Al respecto el profesor Pérez Luño (2005:59) menciona que este cambio se debe a un descrédito en los derechos naturales que tuvo entre los jurídicos alemanes, generando los derechos públicos subjetivos:

“En efecto, la nueva categoría se presentará como intento de ofrecer una configuración jurídico-positiva, de la exigencia mantenida por la teoría de los derechos naturales de afirmar las libertades del individuo frente a la autoridad del Estado. Para eso se precisaba de unas estructuras del poder de forma que fuera posible la instauración de relaciones jurídicas entre el Estado y los particulares, para lo que se debía reconocer la personalidad jurídica del Estado, que de este modo adquiriría la titularidad de derechos y obligaciones para con los ciudadanos, estableciéndose también una consiguiente tutela jurisdiccional de las situaciones subjetivas así instituidas”

La teoría de los derechos públicos subjetivos en principio se formuló para fundamentar la obediencia a la autoridad del Estado, de este derivan todos los derechos y ventajas que concede a los ciudadanos, que son vistos como simples súbditos sin posibilidades de hacer el reclamo alguno. “En otros términos, mientras los derechos subjetivos privados tienen por sujetos a individuos situados en plano de igualdad y que pueden disponer libremente de las facultades que el derecho objetivo les ha conferido, los públicos se desarrollan dentro de relaciones de supremacía/subordinación (...)” (Osuna, 1998:241)

La dimensión normativa de esos derechos públicos subjetivos, en un primer momento aprecia la existencia de una personalidad jurídica del estado, necesario para que este pueda ser un obligado jurídico a no hacer lo que contienen esos derechos y ser luego tutelables judicialmente, en esto coinciden los profesores Néstor Osuna (1998:259) y Alexei Julio(2000:39 y 40).

El ciudadano tiene una serie de pretensiones jurídicas frente al estado, que exige cuando le es incumplida en diversas situaciones jurídicas, frente a las cuales tiene una expectativa definida⁷² que puede exigir contra el Estado, mediante la jurisdicción administrativa. Se tomó la estructura base de los derechos públicos subjetivos para la primera generación de derechos humanos positivizados, así se entendía, como libertades protegidas por el Estado a través de la abstención. Pero las necesidades sociales y económicas que generan cambios en el Estado de Derecho hacen necesario las adaptaciones de esta teoría de las relaciones jurídicas subjetivas, para incorporar los principios básicos del constitucionalismo contemporáneo⁷³.

El profesor Antonio Perez Luño (2005:67-110) explica que los niveles de positivación influyen en la elaboración del catálogo de derechos fundamentales y su forma de

⁷² “En opinión de Jellinek la pertenencia al Estado califica a cada ciudadano y se concreta en una serie de relaciones que lo colocan en diversas situaciones jurídicas (*Zustände*), de las que surgen pretensiones jurídicas (*Ansprüche*). Estas pretensiones de los ciudadanos constituyen los derechos públicos subjetivos, los cuales han ido afirmándose progresivamente en cuatro fases o status.” ((Pérez Luño, 2005:60)

El profesor Néstor Osuna(1998:230) también confirma esta idea al resaltar que “(...) la garantía judicial apunta a la protección subjetiva de sus titulares, cuando ha ocurrido alguna vulneración de los mismos”

⁷³Según Néstor Osuna (1998:253) son: supralegalidad constitucional, rigidez, vinculación general e invocabilidad directa.

consagración. Así a manera de ejemplo, en el nivel constitucional pueden existir enunciados normativos que reconocen libertades o derechos generales, como el derecho a la igualdad, derecho a la libertad derecho a la dignidad humana o bien enunciados concretos que desmenuzan esas libertades generales en aplicaciones prácticas más concretas como la libertad de prensa, libertad de pensamiento, libertad de acceso a la información, libertad de ejercicio profesional; inclusive existen *normas axiológicas o valores*, que consagran aspiraciones de la sociedad y se vuelcan al ordenamiento jurídico para interpretarlo conforme a ellos, *normas instrumentales o de tutela*, que se encargan de fijar los mecanismos para hacer efectivos los derechos y principios generales de la Constitución.

El reconocimiento de la vinculatoriedad de las normas de derecho inicia el debate acerca del tipo de valor que se le dan a las normas de derechos fundamentales⁷⁴. Hay múltiples formulaciones teóricas, desde algunas que le dan un valor *supra-constitucional*, “(...) sus principios tenían como finalidad expresa limitar los poderes del Estado legislador (...) que al constituyente (...) este se limita a constatarlos y proclamarlos solemnemente” (Pérez Luño,2005:75); *valor constitucional*, posición clásica donde se muestra como autolimitación del estado; *valor legislativo*, significando que los derechos fundamentales son desarrollados mediante leyes, una tesis que vació de efectividad a dichos derechos; *valor material*, al expresar que son la guía para la actuación estatal y la interpretación objetiva del derecho positivo (Pérez Luño,2005:78).

Como ambos tipos de derechos subjetivos tienen un núcleo común, la libertad (Pérez,2004:29), es adecuado afirmar que pueden ser entendidos bajo la misma definición de Alexy, como enunciados deónticos, que establecen como correlación un deber de hacer u omitir algo, situación que no enaltece las obligaciones, porque la teoría de los derechos humanos habla de la preeminencia del sujeto para exigir su derecho frente a los demás que se encuentran obligados, es decir, que mi derecho como sujeto preexiste a los deberes que genera cada individuo, pero descontando el hecho de que se encuentran fijados en tratados de orden internacional y no limitados a la Carta Magna.

⁷⁴“El problema de la positivación será visto siempre desde estas premisas no como un acto de reconocimiento o declarativom, sino como un acto de creación y, por tanto constitutivo. Con anterioridad a la positivación podrán reconocerse expectativas de derecho o postulados sociales de justicia, pero nunca derechos” (Pérez Luño,2005:60)

Así la manera de explicar las normas de derecho fundamental y acercarse a su definición se realiza a través de la explicación de su estructura jurídica, partiendo para ello de la teoría de los derechos subjetivos, en especial como la desarrolla el profesor Robert Alexy.

c. Estructura de las normas de derecho fundamental

Si bien los derechos fundamentales tienen unos soportes filosóficos jurídicos bien diferentes: la libertad, la igualdad, la solidaridad, que les hace necesaria una estructura abierta e indeterminada, su concretización debe ser posible para que puedan ser exigibles jurídicamente y responder a las necesidades cambiantes de la sociedad.⁷⁵

Los derechos fundamentales son derechos subjetivos, a pesar de tener una “(...) fórmula semántica abierta, que suelen caracterizarse por su escasa densidad regulativa y por su textura en extremo abierta e indeterminada” (Osuna, 1998:229) y de no ser el sujeto pasivo el Estado exclusivamente.⁷⁶ Modernamente la teoría de los derechos fundamentales⁷⁷ se encarga de estudiarlos.

Conforme a lo dicho anteriormente los derechos fundamentales tienen la estructura siguiente (Alexy, 2007:163): un sujeto obligado indeterminado (b), un sujeto a cuyo favor se constituye (a) a quien se le permite exigir hacer, no hacer o permitir algo (G) que se resume en que: alguien(a) tiene el derecho de exigir que se realice algo (D) a otra persona y quien debe cumplirlo. Se puede representar así:

⁷⁵Es una renuncia al pensamiento encasillado para que los derechos fundamentales puedan renovarse constantemente y no ser algo caducos

⁷⁶ Afirma Néstor Osuna (1998:260): “La contribución de Jellinek estaría agotada, por cuanto sería la noción de derechos subjetivos, como categoría general del derecho, y no su clasificación dicotómica, la que podría tener validez actual.”

⁷⁷Se encarga de analizar la relación de ciertas libertades de acción o derechos ciudadanos, reconocidos positivamente, con el poder estatal y su actividad pública, sobre la base de la jurisprudencia de los tribunales constitucionales de cada país. Robert Alexy (1993:23) acerca de lo que es la teoría de los derechos fundamentales, “Lo que hoy son derechos fundamentales es definido principalmente sobre la base de la jurisprudencia del Tribunal Constitucional Federal. La ciencia de los derechos fundamentales – no obstante la controversia acerca de la fuerza vinculante de las decisiones del Tribunal Constitucional - se ha convertido, en una apreciable medida, en una ciencia de la jurisprudencia constitucional”

<i>DabG</i>	Significa que “ <i>a</i> tiene derecho a que <i>b</i> realice <i>G</i> ” A su vez se deduce del anterior que,
<i>ObaG</i>	Significa que “ <i>b</i> tiene la obligación frente a <i>a</i> de realizar <i>O</i> ”

Alexy (2007:164) explica de la siguiente manera la anterior fórmula: “El objeto de un derecho a algo es siempre una *acción* del destinatario. Esto resulta de su estructura como relación triádica entre un titular, un destinatario y un objeto. Si el objeto no fuera ninguna acción del destinatario, no tendría sentido incluir al destinatario en la relación”

Robert Alexy (1993:27 y ss. Y 2007:32 y ss.) realizó un profundo análisis sobre la definición de norma de derecho fundamental y su estructura. Este trabajo de investigación resume los elementos en:

1. Es un enunciado normativo⁷⁸-semántico⁷⁹ de carácter deontológico⁸⁰.
2. Se encuentran en la constitución (criterio formal) para conferir derechos subjetivos(criterio material) y estar dentro del mismo fundamento del estado(criterio material); “(...) son sólo aquellas que son expresadas directamente por enunciados de la LF(disposiciones de derecho fundamental)”(P.66)

⁷⁸ Afirma el profesor Robert Alexy(2007:31) : “Siempre que alguien tiene un derecho fundamental, existe una norma válida de derecho fundamental que le atribuye ese derecho”

⁷⁹ Dice el profesor Robert Alexy (2007:34 y 55) sobre el carácter semántico del enunciado de una norma de derecho fundamental: “El hecho de que la misma norma pueda ser expresada por medio de diferentes enunciados normativas, pone de manifiesto que hay que distinguir entre el enunciado normativo y norma”

“Cada cual puede afirmar con respecto a cualquier norma, que ella debe ser adscrita a la disposición de derecho fundamental. No obstante, s afirmación acerca de la existencia de norma de derecho fundamental tendrá como objeto una norma de derecho fundamental si se lleva a cabo conforme a derecho”

⁸⁰Sobre el carácter deontológico dice Robert Alexy en su nota al pie 14(2007:37): “Hay que subrayar que los enunciados deónticos no son algo diferente de los enunciados normativos, sino una clase parcial de los enunciados normativos”

3. Algunas son integradas o concretizadas para casos específicos, por ello se les llama normas adscritas de derecho fundamental, Otras, son estatuidas directamente del texto constitucional.⁸¹
4. Requieren de una fundamentación correcta para que sean válida, expresar argumentos fuertes “(...) que sea posible aducir a su favor” (Alexy.2007:54)
5. Tienen una estructura que las define como principios que conceden derechos a algo, libertades o competencias.

El análisis que realiza respecto a la estructura de las normas de derecho fundamental termina definiéndolas como enunciados normativos (Alexy, 2007:47 y ss.) que establecen posiciones jurídicas que reconocen algo frente al otro, entendido este como el Estado o las personas jurídicas o naturales. Las posiciones que concibe Alexy 2007: 163) pueden ser clasificadas en *derechos a algo, libertades y competencias*.

El concepto de norma fundamental, bajo la perspectiva que Alexy propone, tiene una estructura compuesta de: principios y reglas (Alexy, 2007:63) que se manifiesta de dos maneras posibles en la Constitución: como *principio* cuando “(...) ordena que algo sea realizado en la mayor medida posible, dentro de las posibilidades jurídicas y reales existentes (...) ”(Alexy,2007:67), es decir, que hay posibilidad de “jugar” y argumentar, en su iusfundamentación, el grado de cumplimiento según los casos y enfrentamientos que ocurran; como regla cuando no da otra posibilidad más que actuar conforme a ella o no actuar conforme a ella(Alexy,2007:68).

⁸¹“Ellas son necesarias cuando debe aplicarse a casos concretos la norma expresada por el texto de la Constitución. Si no se presupusiese la existencia de este tipo de normas, no sería claro qué es aquello que, sobre la base del texto constitucional(es decir, de la norma directamente expresada por él), está ordenado, prohibido o permitido”(Alexy, 2007:52)

d. La importancia del estado social de derecho en las normas de derechos fundamentales

La titularidad de los derechos y su eficacia ante terceros ha sido un problema surgido a raíz de la proyección vinculante de la Constitución sobre todos los ámbitos del derecho y el abandono de la aplicación de los derechos fundamentales exclusivamente a las relaciones entre el estado y los particulares.⁸²

La justificación principal es que la Constitución no es sólo un conjunto de normas de contención al poder estatal sino también de normas que ordenan e intentan corregir los desequilibrios en las relaciones sociales particulares; según Pérez Luño(2005:96) la eficacia de los derechos fundamentales se justifica en que “(...)suponen la consagración jurídica de unos valores que por su propia significación de básicos para la convivencia política no limitan su esfera de aplicación al sector público o privado, sino que deben ser respetados en todos los sectores del ordenamiento jurídico”.

Sobre la importancia de la expedición de normas que desarrollen los derechos fundamentales habla Pérez Luño(2005:105,234-235) lo siguiente:

“El estado social de derecho implica también la superación del carácter negativo de los derechos fundamentales (...) lejos de implicar un debilitamiento de las garantías de la libertad individual, inherentes al concepto clásico del estado de derecho”

Los derechos fundamentales entran en relación con el principio de legalidad cuando se le confiere al legislador la tarea de concretarlos en el ordenamiento jurídico, obsesionados los primeros constituyentes de limitar por la ley el poder absoluto del ejecutivo con derechos universales y absolutos (Pérez Luño, 2005:318-322). Sin embargo la preocupación por la

⁸²“El realismo más elemental obliga a reconocer que las libertades puras, aquellas cuyo disfrute sólo dependería de la abstención del Estado, se hallan irremediamente superadas por la evolución económica y social de nuestro tiempo. ¿Qué sería – se pregunta Burdeau – de la libertad de circulación sin un código del tráfico, de la libertad de cultos sin las subvenciones, para el mantenimiento de los templos, de la libertad de prensa sin privilegios fiscales para los periódicos(...) (Pérez Luño, 2005:93)

pérdida de soberanía popular, que pasaba a estar en cabeza el órgano representativo, hizo palpable la necesidad de diseñar técnicas interpretativas para conversar el rango superior de los derechos fundamentales frente a las normas legales que las desarrollaban, a través del control jurisdiccional de estas. El estado de Derecho (Pérez Luño, 2005:100 y ss.) fue un gran impulsor de la positivización de los derechos fundamentales, pero su apego al dogma de la ley lo transformó a otro modelo de estado más permeable a las necesidades sociales y humanas que se denominó estado social de derecho.

A principios del siglo XX se formulan como derechos públicos subjetivos, remarcando su carácter normativo positivo de las libertades que le reconoce el estado (Pérez Luño, 2005:58-61). Durante ese mismo tiempo se realiza una crítica por la concepción tan formalista que implicaba el reconocimiento estatal de los derechos, sin detenerse en mecanismos o procesos para la protección efectiva. Las tres escuelas teóricas mencionadas permiten deducir que el proceso es reconocer el derecho y diseñar los mecanismos de protección y disfrute del derecho. Resuenan las palabras del profesor Costas Douzinas acerca de la lucha por los derechos es una lucha por la autorrealización: “De otro lado – el lado de los empíricos -, los derechos fueron, desde su inclusión en la experiencia política de la libertad, la expresión de la lucha para liberar a los individuos de la coacción externa, permitiendo así su autorrealización” (Douzinas, 2007:6)

Clasificación del Habeas Data

El derecho tiene una labor importante para dar una confianza a las personas que conviven a diario y ser al mismo tiempo una herramienta para hacer cumplir las normas. Es una labor de contención y reacción.

La prevención ante el impacto que causó la invención de la tecnología en el abaratamiento de la capacidad de almacenamiento y procesamiento de datos personales hace necesario crear un derecho especializado que intenta orientar todos los fenómenos posibles y dar unas pautas generales de conducta obligatoria. En este caso frente a este nuevo poder

informático el derecho no deja desprotegidos a las personas y le otorga diferentes clases de herramientas jurídicas para luchar por la protección de cada uno de sus derechos vulnerados.

Los derechos protegidos con las herramientas jurídicas, que se agrupan bajo el nombre de Habeas Data, pretenden dar una “protección inmediata y efectiva a los derechos fundamentales afectados por las prácticas de almacenamiento, procesamiento y suministro de datos”(Puccinelli, 2004:476) y se regularon a distintos niveles: constitucional, legal y administrativo. El nivel de regulación impacta en los efectos de protección, puesto que a mayor superioridad jerárquica en el ordenamiento jurídico de cada país se hace más exigible y se presta más atención a las vulneraciones de las normas.

Ahora bien según el derecho que se pretenda proteger o ejercer con cada acción el profesor Oscar Puccinelli (2004:487) propone una clasificación del Habeas Data, que se fundamenta en lo propuesto por el profesor Néstor Sagües. La Corte Constitucional colombiana desglosa los tipos de habeas data como facultades de las personas para: “(...) solicitar y obtener, en un tiempo razonable, la corrección, complementación, inserción, limitación, actualización o cancelación de un dato que le concierne.”

Los criterios que tiene en cuenta para una clasificación inicial son (Puccinelli, 2004:488-489): la finalidad, el momento de inicio de la acción, los efectos de la sentencia que produce la acción y los alcances de la legitimación por activa. En el primer criterio se centra en lo que desea conseguir (acceso, bloqueo, exclusión, rectificación), se denomina *habeas data propio*, para prevenir o reparar lesiones de derechos propios, y *el habeas data impropio*, para acceder a información pública o difundir información; el segundo criterio es al momento de incoarse la acción y la tutela que persigue sobre sus derechos, significa que será *habeas data preventivo* si ocurrió antes de la lesión del derecho y *habeas data correctivo o reparador* cuando la lesión está consumándose o de haber terminado se pretende un resarcimiento; como tercer criterio tenemos los efectos de la acción, interpartes o erga omnes; el cuarto criterio se refiere a la cantidad de legitimados por activa para iniciar la acción, siendo *habeas data individual*, uno solo o sus sucesores y *habeas data colectivo*, cuando son muchos y uno solo los representa.

a) *Habeas Data Propio*

Este tipo de acción opera para los encargados y responsables de bancos de datos que realicen el tratamiento de datos personales para obtener el respeto a los derechos ARCARs o exigir que se reparen los perjuicios causados a raíz del tratamiento. Sus dos subtipos son *preventivos, correctivos y reparadores*.

El *Habeas Data preventivo* se inicia para ejercer los derechos de acceso y conocimiento y obtener la información necesaria acerca de lo que se conoce de nosotros, la finalidad por la cual nos han pedido los datos, las condiciones bajo las cuales se obtuvieron los datos o por tenerse indicios de una vulneración en algunos de los principios. Los subtipos de este habeas data son: *localizador, finalista, exhibitorio y autorial*.

El *habeas data localizador* pide que se conozca la existencia y ubicación de los bancos de datos, para identificar quienes son el responsable y encargado ante las reclamaciones que hagan los titulares. También busca indagar acerca del origen de los datos personales que conciernen a una persona y concluir si hay consentimiento para haber realizado el uso de los datos personales. El *habeas data finalista* se propone conocer “(...) si las categorías de los datos almacenados se corresponden con la finalidad declarada (...)” por el responsable de la base de datos. El *habeas data exhibitorio* pretende que se dé información acerca de los datos que se encuentran almacenados en las bases de datos.

El *Habeas Data correctivo* tiene la función de detener el tratamiento de datos personales para incorporar o modificar datos personales, sin lo cual puede convertirlo en ilegítimo o ilegal y vulnerar derechos del titular. Se ejercitan los derechos de rectificación o actualización. Dentro de estos tenemos el *aditivo, rectificador, cancelatorio, encubridor*.

- El *Habeas data aditivo* busca incorporar datos personales que son necesarios para realizar el tratamiento acorde a la finalidad, por ejemplo cuando modificamos nuestro perfil en una red social o solicitamos que nos incluyan en algún programa beneficiario del

Gobierno⁸³; será actualizador cuando pagamos la octava cuota de un crédito a doce meses nos comenta la cajera que no hemos consignado el valor de las cuotas 4 y 5, así que nosotros debemos presentar los recibos de pago de esas cuotas y actualizar el dato viejo acerca de la cantidad de dinero que se debe por una obligación comercial o financiera. Será *aclaratorio* cuando se piden incluir datos adicionales para evitar que en el tratamiento se interprete incorrectamente la situación, por ejemplo, que un banco de datos confunda al garante de la deuda con el deudor principal. Por otro lado será *inclusorio* cuando deba incluirse un dato importante para evitar sanciones o confusiones al respecto.

- El *Habeas data rectificador* busca corregir los datos porque estos son falsos (carece de verdad total, diferente de los datos caducos que fueron ciertos en un tiempo pero ahora ya no lo son) o imprecisos (da lugar a varias interpretaciones potencialmente vulneradoras). Un ejemplo de esta situación ocurre cuando a una persona le niegan un préstamo porque tiene un crédito en mora y está reportado en una central financiera por una tarjeta de crédito que uso y no pagó. En este caso deberá demostrar las condiciones bajo las cuales el no pudo haber hecho uso de la tarjeta: estaba suspendida por renovación, se la habían hurtado para la fecha en que se realizó el préstamo, no realizó la autorización de que le expidieran una.
- El *Habeas data cancelatorio o excluyente* busca “eliminar total o parcialmente los datos almacenados respecto a determinada persona, cuando por algún motivo no deben mantenerse incluidos en el sistema (...)” (Puccinelli, 2004:493), esos motivos pueden ser la desactualización del dato, la falta de consentimiento para el tratamiento o la calidad de dato sensible que la hace intratable por cualquier mecanismo.

⁸³Ver Sentencia T-307 de 1999 MP Eduardo Cifuentes Muñoz: “Ahora bien, el derecho de acceso a los bancos de datos no cuenta exclusivamente con una vertiente negativa. Es probable que una persona no quiera que un dato que le concierne forme parte de un banco de datos, pero puede ser que, por el contrario, la inclusión del mencionado dato resulte de su interés. En este caso, corresponde a la ley definir, conforme entre otros, a los principios de igualdad y no discriminación, los eventos en los cuales una persona tendrá derecho a que se incluya en un determinado banco de datos cierta información que le es propia. La vertiente positiva del derecho de acceso a los bancos de datos se encuentra, en principio, supeditada a la reglamentación legal que al respecto se expida para cada sector.”

- El *Habeas Data encubridor* busca que cierta clase de datos personales no se muestra a todo el público o no sea accesible por toda la operación de tratamiento de datos, debiéndose fijar las políticas técnicas para el efecto. Los siguientes son tipos de habeas data: *reservador, disociador, encriptador, bloqueador, asegurador*.

El Habeas data reservador busca que un dato correcto, consentido y legítimamente almacenado se mantenga confidencial y se comunique a los que haya autorizado o bajo ciertas condiciones.

El habeas data disociador busca que cierta información no se asocie a una persona sino a un grupo grande, así se vuelve anónima la identidad de la persona. (Puccinelli,2004: 494)

El habeas data encriptador busca seguridad al dato almacenado, usando procedimientos de encriptación para evitar que en una filtración pueda conocer toda la información personal.

El Habeas data bloqueador busca que no se realice ninguna clase de tratamiento con terceros del dato personal o que se transmitan o que conozcan. Se ordena como medida cautelar o definitivamente en sentencia, de manera subsidiaria ante la negativa de cancelar el registro del dato.

El habeas data asegurador pretende que se modifiquen las condiciones técnicas de protección del dato personal en su tratamiento para que cumplan con la norma.

El *Habeas Data reparador* busca la reparación del daño moral o patrimonial causado. Se ejerce el derecho de oposición. Tenemos el impugnativo y el resarcitorio. Será impugnativo cuando el titular se opone a las decisiones que se tomen a partir de los datos personales que conozcan o tengan almacenados de él para buscar que se elimine o se cambie. Por otro lado será resarcitorio cuando sólo se busca la reparación de los perjuicios, el daño patrimonial o moral causado con el tratamiento.

b) Habeas Data impropio

Busca acceder a la información pública que el estado tiene, excluyendo aquellas que no pueden conocerse inmediatamente sino pasado un tiempo y son reservadas por diversos asuntos.

c) Habeas Data individual

Ejercido por una persona jurídica o natural de manera individual, por sí misma o por representación de abogado.

d) Habeas Data colectivo

Representa la acción para proteger un grupo de personas grande frente al tratamiento indebido o que se encuentran en trance de ser afectados. Se tutela este derecho cuando son muchos los afectados por un responsable o encargado de tratamiento de datos personales. Algunos países asignan la función al defensor del pueblo, a asociaciones de derechos humanos, etc.

Justificación para la protección jurídica con herramientas específicas

“[L]a libre eclosión de la personalidad
Presupone en las condiciones modernas
de la elaboración de datos
la protección del individuo (...) de los datos
Concernientes a la persona”
Tribunal Constitucional alemán,
Sentencia Caso del Censo de 1983

Garantía de la dignidad humana a través del respeto al Habeas Data

Todo el derecho al debido tratamiento de datos personales así como los derechos de la personalidad se enmarcan en el individuo liberal, a quien se le concibe como una persona que toma sus decisiones y es el fin y fundamento de todo el actuar político y estatal. Resaltar al individuo implica reconocerle una proyección en el mundo jurídico que se realiza mediante la dignidad humana, cuya formulación filosófica se debe a Inmanuel Kant, quien lo fundamentó como algo intrínseco al ser humano, que le da el suficiente valor propio para que no sea utilizado como instrumento para los fines de otra persona.

La dignidad humana reconoce a las personas su calidad de ser humano, les concibe en su totalidad como individuos que merecen ser respetados en su integridad, en sus creencias y en sus actividades desplegadas en la realidad. Esto es patente desde el momento en que en la Edad Media comienza a separarse de la comunidad que la reconocía sólo a ciertos roles (dignidad como sinónimo de rango o abolengo) y luego se generaliza, cuando se formula que cada persona tiene una pequeña chispa divina que le da un rol específico (dignidad humana como respeto al mismo ser supremo). Posteriormente se hace el reconocimiento de otras facultades que sirven para la búsqueda de lo que el creador desea para nosotros, lo que conlleva a que nadie pueda impedirnos que emprendamos esa búsqueda o utilizarnos para sus fines personales porque iría contra esos designios (dignidad como autonomía individual inherente a nosotros y diferenciador de otros animales).⁸⁴

⁸⁴Según Peces-Barba (2013:173 -174.) este es sólo el primer rasgo de un total de seis que identifica en las concepciones de los filósofos.

En la época moderna se quita la intervención divina de nuestros destinos y se afirma que simplemente el hombre debe tener el derecho de darle sentido a su vida, para ello debe respetársele el ejercicio de su libertad como desee y sin impedimentos u coacciones para hacer otra cosa. La ética kantiana afirma que el hombre es por esta razón alguien digno, es un fin en sí mismo.

Existe una relación de legitimación entre el principio de la dignidad humana y el Estado Social, Constitucional y Democrático de Derecho, la razón fundamental está en lo que significa la Dignidad Humana para la actuación estatal: i) Implica cumplir una serie de medidas que permitan garantizar de la mejor manera posible el ejercicio de la libertad, con políticas distributivas o mecanismos de tutela de los derechos fundamentales en comunidad ii) Incorporar a la acción estatal la promoción de la capacidad de decisión y configuración de su existencia en el hombre y iii) Reconocerle para el ejercicio de su autonomía una serie de posiciones y situaciones jurídicas permanentemente protegidas a través de la organización judicial. De esta manera todo el Estado se instrumentaliza para que esté al servicio de la autonomía del ser humano y sus derechos fundamentales, sin perder de vista la orientación comunitaria del bienestar general que impera en el Estado social de derecho.

Los derechos humanos son vinculados directamente con el ser humano, en razón a que reconocen un valor intrínseco con la propia existencia de la persona, quien no puede ser concebido como un instrumento sino como fin en sí mismo y usa su razón para descubrir cuál es. Esto permite fijarle como uno de los fundamentos de los derechos humanos y reconocer los derechos de la personalidad. Es una inquietud que se ha profundizado en la doctrina jurídica y la filosofía del derecho, intentando darle al mundo y la sociedad caracteres más “humanos”.⁸⁵El derecho a la intimidad forma parte del conjunto de los derechos de la personalidad.

⁸⁵ “Si la lucha por el reconocimiento de la dignidad de la persona humana puede considerarse como una constante en la evolución de la filosofía jurídica y la política humanista, la tendencia a la positivación de las facultades que tal dignidad entraña se puede considerar como una inquietud estrechamente ligada a los planteamientos doctrinales de la hora presente”(Pérez Luño, 2005:55)

El derecho a la intimidad permite ese espacio reservado, en el que la persona desarrolle internamente sus valores importantes, analizando de manera tranquila las circunstancias que le rodean. El individuo toma sus decisiones fundamentado en el plan de vida que quiere tener, esa reflexión queda reservada al espacio propio de él. En el seno del pensamiento anglosajón el concepto de *privacy* tuvo un presupuesto teórico inmediato en la idea de libertad como autonomía defendida por John Stuart Mill en su trabajo *On Liberty* (Pérez Luño, 2005:329). Sin embargo, hay conductas que tienen relevancia pública, lo que significa que están excluidas del ámbito de protección esencial que se relaciona con la dignidad humana. “Precisamente estos rasgos del carácter y de la persona son objeto de la curiosidad pública y privada (...) Pero asimismo es digno de protección el interés del Estado en cumplir los cometidos que le encomienda la Constitución. Y al respecto no son excluibles colisiones con las expectativas a protección de la esfera privada” (Benda, 2004:129 y 130)

Al respecto la Corte Constitucional de Colombia en Sentencia T-414 del 16 de junio de 1992, Magistrado Ponente Ciro Angarita Barón, planteó la vinculación a la personalidad y la dignidad del ser humano cuando dice que

"(...) se protege la intimidad como una forma de **asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas**, vale decir, como un derecho de la personalidad.

Esta particular naturaleza suya determina que la intimidad sea también un derecho general, absoluto, extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer "erga omnes", vale decir, tanto frente al Estado como a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada. Su finalidad es la de asegurar la protección de intereses morales; su titular no puede renunciar total o definitivamente a la intimidad pues dicho acto estaría viciado de nulidad absoluta".

"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 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, aparece en primer término el respeto a la dignidad humana" (negrilla fuera de texto)

El derecho a la protección de datos personales se vincula profundamente con la garantía de la dignidad humana porque permite la autodeterminación informática o informativa, el ejercicio de la potestad de configuración propia a partir de lo que se desea y como se es visto a sí mismo y no a partir de lo que la sociedad y el Estado concluyen que podemos ser, apoyados en la información que tienen de nosotros. Cuando se destruye la intimidad o privacidad, el afectado pierde control de la transmisión de la información personal, pasa de ser influido a ser influenciado, de ser un fin en sí mismo a ser un objeto productor de información, un medio para lograr los fines de las organizaciones privadas y públicas. Concluye esta sección con la siguiente idea tomada de la sentencia 254 de 1993 proferida por el Tribunal Constitucional español: "Derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos"

Apropiación de la personalidad por la sociedad de la información

El derecho a la intimidad se concibió para dejar un espacio en soledad a la persona, que nadie debía entrar sin permiso. Las personas se encargaban de dar ese permiso para que cualquiera ingresara a esa esfera tan privada e íntima. Pero la época actual de avances tecnológicos y comunicacionales que trajo el internet genera un retroceso en los ámbitos de protección la intimidad. (cfr. Pérez Luño, 2006:131 y ss.)

La preocupación comenzó después de que se conociera el uso de la computación para procesar la información de las personas en la Segunda Guerra Mundial, separando a los que son judíos de quienes no, a través d capacidad de analizar y procesar todos los datos dispersos sobre las personas para apoyar el programa de superioridad racial del gobierno nacional-socialista (en este sentido cfr.Con CE, 2007:5). Las personas ante este hecho, y la expedición de leyes de empadronamiento similares, comienzan a interrogarse acerca del uso que están haciendo entidades gubernamentales⁸⁶ y compañías privadas sobre la información que ellos decidieron entregarles y que concernia a su identidad y personalidad (Pérez Luño, 2006:88 y ss.).

En los años 60 a 70 las tecnologías, iniciales que surgen con la computación, facilitan una mayor captura de datos de las personas (poder informático), y ponen al individuo como objeto de decisiones o conductas privadas o públicas que pueden afectarle, es un nuevo dominio social. “La posibilidad de injerencias en la intimidad se incrementaba así de forma espectacular, y el legislador no podía ser ajeno a esa nueva realidad que emergía de modo irrefrenable” (Piñar, 2003:47)

El siglo XXI es la era de las Tecnologías de la Información y las Comunicaciones, porque se ha permitido que se administren y transmitan grandes cantidades de información en tiempo real⁸⁷, sin límites, lo cual acentúa algo que ya estaba presente a mitad de los años cincuenta: construir un perfil de las personas acerca de sus condiciones individuales, de sus preferencias y posibles orientaciones a futuro. Al respecto la Corte Constitucional, de manera anticipatoria en sentencia T-729 de 2002, proyecta que la sociedad de la información se tomará la vida de todos los colombianos y bien podrá representar un peligro cuando se use de manera discriminada:

“Ante el surgimiento del poder informático, la existencia de un número único de identificación de los nacionales colombianos se ha constituido hoy en un factor de riesgo para el ejercicio de los derechos fundamentales. Esta situación se hace evidente, ante la

⁸⁶En el presente tenemos los sistemas de seguridad e interceptación de las comunicaciones, por ejemplo el *Echelon* o el *Carnivore* , que se diseñan con el ánimo de apoyar a la lucha contra el delito previniendo su ocurrencia, a la manera de la película *Minority Report*, pero terminan siendo usados para control social de las personas, violando su intimidad (Pérez Luño, 2006:97-101)

⁸⁷ Un cruce de información con otras bases de datos públicos o privadas adquiridas son ejemplos del cruce relacional de información

relativa facilidad de efectuar los llamados “cruces de datos”, de tal forma que con la digitación de un solo dato (el número de identificación) y la disponibilidad de varias bases de datos personales, es posible en contados minutos elaborar un “perfil virtual” de cualquier persona.

Todos esos datos son conseguidos gracias al Internet, las aplicaciones web y móvil y últimamente los smartphones; tecnología que abre la puerta a una aldea global, pero también hace pensar en la necesidad de obtener una regulación beneficiosa para los inocentes ciber-ciudadanos que entregan sus datos a cambio del uso de productos y servicios, inconscientes acerca del uso posterior que se les dará o quizá si conscientes del uso que le dan sin darle importancia a las consecuencias futuras: i) una restricción grande en el derecho a la información libre, cuando se le muestran acontecimientos o ideas que van acorde a las preferencias y se omiten otras que pueden representar una amenaza para ciertos gobiernos o ii) un acceso abusivo a sus datos mediante técnicas no invasivas de sus correos, dispositivos y servidores para juzgar lo que están haciendo(en este sentido sobre las facilidades de violar la intimidad cfr. Pérez Luño,2006:103).

Esa apropiación de la identidad virtual, que se consigue con los trabajos de análisis y relación de muchos datos personales, es una preocupación que expresa el interés de tutelar jurídicamente con mayor fuerza la intimidad y la vida privada, mediante el otorgamiento de herramientas que den “dientes” a las personas para evitar la apropiación indiscriminada de sus datos personales en cabeza de los sujetos responsables de las bases de datos; “la necesidad de su ordenación”aumentará al ver que debemos dar datos personales si queremos recibir servicios satisfactorios, sin obtener garantías acerca del uso para el fin establecido⁸⁸.Esto conduce a una problemática mayor, como es la eficacia de los derechos fundamentales frente a terceros, que se tocará tangencialmente infra⁸⁹, en la medida que importa para los efectos de que puedan impetrarse los mecanismos ante los particulares por violación de derechos fundamentales.

⁸⁸En este punto el profesor Antonio Pérez Luño (2006:103), en cuanto a la regulación jurídica del Internet, le parece recordar los debates de los filósofos de la modernidad acerca de la preferencia entre el estado de naturaleza o el estado de derecho.

⁸⁹Ver supra. 1.4.3. Herramientas jurídicas para la protección de datos personales.

La potencial amenaza que representan las nuevas tecnologías genera una reacción del derecho para prevenir los usos perjudiciales e indemnizar por los daños que generaron los antiguos sistemas de registro de base de datos, los sistemas de información, y ahora los modernos software de distinta clase, entre los que destacan las “Apps” por ser de uso común en los dispositivos modernos de comunicación celular que portan millones de personas consigo.

Hay una nueva faceta surgiendo del derecho a la intimidad que no niega la intromisión en la vida privada y da una facultad jurídica a las personas para controlar el uso de los datos y evitar o evidenciar las violaciones producidas. Para el profesor Nelson Remolina (1994:198) actualmente se presentan dos tipos de violación de la intimidad: i) acceso inadecuado o sin permiso a la información de la persona o a su esfera personal, con técnicas para obtener la información o con software o hardware de grabación de la voz o de la imagen o combinados; ii) Abuso del permiso otorgado, cuando la persona autoriza para un fin determinado pero se da cuenta de que se utilizó para otros no incluidos. Esta nueva faceta es el derecho al debido tratamiento de datos personales.

Necesidad de equilibrar la balanza frente al poder informático

Las legislaciones que han reaccionado inicialmente, para proteger la intimidad y el debido tratamiento de los datos personales, han sido las de Estados Unidos y Europa. Cada uno de ellas con sus peculiares características ha puesto en vigencia regulaciones jurídicas, que los otros países del mundo siguen con mayor o menor fidelidad.

La antigua noción de Warren y Brandeis ha sido replanteada en el presente, analizándose no solo las influencias externas en nuestra vida privada sino los alcances que tiene está en nuestras relaciones sociales, piénsese por ejemplo en la importancia que trae el prestigio de un profesional para que se le contrate en determinada obra. Inicialmente se intentó contener dándole una nueva faz al derecho a la intimidad “(...) que la reivindica de su inicial cariz individualista y negativo. Se trata, ni más ni menos, de reconocerle un espacio propio entre las denominadas libertades públicas, vale decir, entre aquellos derechos fundamentales de una

sociedad que permiten el desarrollo y mantenimiento de la personalidad y la dignidad humana”. Al respecto el profesor Pérez Luño (2006:131) piensa que la intimidad como soledad es la primera etapa de la noción actual.

La segunda etapa comienza cuando hacemos vínculos sociales con otras personas y nos comunicamos dando información (señas, datos, descripciones), se reconocen los derechos de conocer, acceder y controlar las informaciones que conciernen a cada persona, la intimidad se transforma en *autodeterminación informativa*.⁹⁰ El Tribunal Constitucional Federal de Alemania concluye en la sentencia de 15 de diciembre de 1983 que es una facultad de controlar la divulgación y utilización de los datos referentes a una persona, deducible a partir del derecho a la personalidad que entiende como “(...) la libertad de decisión sobre las acciones que vaya a realizar o, en su caso a omitir, incluyendo posibilidad de obrar de hecho en forma consecuente con la decisión adoptada” (Boletín de Jurisprudencia Constitucional, 1984:153)

Ese derecho reconocido en cabeza de cualquier persona se estableció para evitar el surgimiento de lo que Cerda (2003:52) llama “dictaduras tecnológicas”, que bajo la buena excusa de conocer lo más que puedan de sus ciudadanos, para ofrecerles la mayor realización espiritual, determinan lo que cada uno de nosotros “queremos” conocer o hacer, inclusive sin que debamos facilitar constantemente nuestros datos personales más característicos (cfr. CE, 2007:15). “En efecto, desde que la información personal denota valores personales, la prevención frente a su tratamiento no suscita solo problemas individuales, sino conflictos que importan a la sociedad en su conjunto, porque el uso de la información permite controlar y coartar el comportamiento ciudadano” (Pérez Luño citado por Cerda, 2003:53).⁹¹ Se generan unas auténticas relaciones de poder, que en términos de Norberto Bobbio (1998:133) implica

⁹⁰La Corte Constitucional colombiana concluye lo mismo en el párrafo segundo de las consideraciones 2.6.3 de la sentencia C-748 de 2011: “(...) las limitaciones propias del derecho a la intimidad no son suficientes para responder a las necesidades del flujo de la información moderna. Por el contrario, se está ante el nacimiento de un nuevo derecho, el de habeas data, en el que la privacidad “no implica sencillamente la falta de información sobre nosotros por parte de los demás, sino más bien el control que tenemos sobre las informaciones que nos conciernen”

⁹¹En eso coincide también la Corte Constitucional colombiana en sentencia T-414 de 1992: ““Por las características propias de los datos, una vez producidos (codificado un evento u objeto por alguien o eventualmente una máquina) pueden diseminarse con relativa facilidad. Esto hace que puedan ser usados, en combinación con otros de procedencias distintas pero adscribibles a la misma persona. Así se va configurando lo que ha dado en llamar un “perfil de datos de una persona”(Lleras). Estos perfiles pueden construirlos quienes tengan bancos de datos bien sea manuales o sistematizados, y el poder de información y control social que estos tengan depende del uso de la tecnología disponible.”

que “un sujeto condiciona y en tal sentido hace no-libre el comportamiento del otro (...)”, generando en cabeza de los creadores de bases de datos un poder informático, fundamentado en la nueva capacidad de condicionar a las personas a través de la percepción que la sociedad tiene de ellas, lo que configura un poder ideológico, esta es una de los medios principales que enunciaba el maestro italiano Bobbio(1998:133)

La sentencia que lo estructura jurídicamente viene del Tribunal Constitucional Alemán quien se pronuncia el 15 de diciembre de 1983 con motivo de la ley del censo de la población de 1982. Comienza contextualizando como el avance de la tecnología ha hecho fácil que se genere una imagen pormenorizada de cualquier hombre, sin embargo este se encuentra a merced de los entes que hacen uso de esas técnicas porque se ha vuelto un requisito esencial para entrar en relaciones jurídicas con el Estado y los particulares; el Tribunal Constitucional Federal de Alemania para darle la tutela jurídica reconoce que las personas tienen el derecho de decidir y disponer libremente sobre sus datos y quien pueda acceder a ellos. Es destacable que señalara la imperiosa necesidad de mecanismos jurídicos para guardar efectivamente el derecho fundamental.

El derecho de la protección de datos personales se justifica por la contaminación de las libertades clásicas a través de nuevas maneras y medios, que no cabrían adecuadamente dentro del derecho general de la intimidad; se tiene el ejemplo de independencia que existen de los derechos a la honra, al buen nombre y a la imagen, así se independiza un nuevo derecho totalmente de la intimidad⁹². Esta independencia no significa un corte o separación radical puesto que el indebido tratamiento a los datos personales afecta directamente a la intimidad y los otros derechos al buen nombre o la honra e indirectamente perjudica la dignidad humana. Como lo dice la Corte Constitucional colombiana:

“Esta reciente garantía requiere entonces del reentendimiento de instrumentos de tutela jurídica y de ciertos principios que respondan a las necesidades del control del manejo de datos. En efecto, se enfrentan dos intereses, por un lado, la especial necesidad de

⁹²Para el profesor Nelson Remolina (2012:5) ambos derechos son independientes porque el “(...) primero [habeas data] otorga “facultades positivas de disposición y control” de los datos personales, mientras que el segundo [intimidad] confiere “facultades negativas de exclusión y terceros” de la vida privada y familiar de una persona.”

disponibilidad de información mediante la conformación de bases de datos personales, por otro, el requerimiento de proteger los derechos fundamentales de los posibles riesgos del proceso de administración de datos. En consecuencia, se torna indispensable someter este proceso a ciertos principios jurídicos, con el fin de garantizar la armonía entre las relaciones jurídicas.”(Sentencia C-748 de 2011 MP Jorge Pretelt Chaljub)

Así Cerda Silva (2003:55 y ss.) menciona que la jurisprudencia constitucional española ha interpretado en la constitución de ese país que existe un derecho a la autodeterminación informática, lo que permite a las personas ejercer un estricto control de los datos almacenados por programas informáticos o mecánicos en bases de datos.

Las normativas nacionales, regionales e internacionales empiezan a elaborar enunciados normativos reconociendo esta libertad informativa o dando ciertas recomendaciones a sus países miembros para que adapten sus ordenamientos jurídicos a las nuevas circunstancias tecnológicas. A nivel internacional la norma más destacada es la Resolución de la ONU n°45/95 de 1990 sobre principios rectores para el tratamiento de ficheros computarizados.

La jurisprudencia constitucional colombiana fijó una aproximación inicial en su sentencia T-414 de 1992, donde concibe la necesidad de controlar el poder informático en ejercicio de la libertad a través de la protección de la intimidad, que se proyecta en el uso de las tecnologías para “(...) 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. “

En una última fase aparece la preocupación de diseñar mecanismos que tutelen jurídicamente los nuevos derechos reconocidos y permitan ejercer una supervisión por una autoridad asignada ante la desestimación de las peticiones o solicitudes realizadas por las personas a las entidades responsables o encargadas del tratamiento. Al respecto Alberto Cerda Silva (2006:235) afirma:

“El control (...) supone la concurrencia de dos elementos esenciales: existencia de un determinado estándar normativo conocido para el agente controlador como a quien se supervisa y el segundo, la formulación por el agente de control de un juicio de adecuación de la actividad de quien es controlado a tal patrón. Ese patrón o estándar normativo junto al juicio se conjuga en los mecanismos de control que verifican el cumplimiento así como también sancionan, son preferiblemente judiciales, aunque no se omiten los administrativos”

La razón de ser de los mecanismos creados para el titular del dato es garantizar el derecho efectivo a la autodeterminación informativa, citando a Pérez Luño el autor fija en que hay una “procedualización del derecho moderno”. Siguiendo la anterior tónica algunos estados crean un procedimiento específico, concentrado y simplificado. La doctrina denomina *habeas data*, tomando prestado de *habeas corpus*⁹³ algunas características, y hace referencia a la acción propiamente como al proceso que inicia el titular del dato. (Requerimiento de sus datos-reclamación administrativa-acción judicial). Pero en Europa se incluye el recurso judicial como los otros mecanismos para garantizar y ejercer sus derechos ARCO de carácter administrativo.

Eficacia de los derechos fundamentales entre particulares

La justificación principal para proyectar los derechos fundamentales sobre las relaciones privadas o particulares se debe al profundo interés de superar los obstáculos presentados en el ejercicio de los derechos fundamentales por parte de los ciudadanos, pues es una limitación grave a la igualdad material no obtener en esta sociedad actual los bienes básicos, sabiendo que existen otros círculos de influencia que lo impiden y que se encuentran fuera del Estado (Pérez Luño, 2005:96). Esto se conoce como la teoría de la eficacia de los derechos fundamentales frente a terceros o frente a personas diferentes al Estado⁹⁴. El profesor Antonio

⁹³Semejante en cuanto a que ambos logran que se respete la libertad del cuerpo y de la información respectivamente. Permiten el ejercicio de la libertad física y moral.

⁹⁴Para profundizar en los debates doctrinales y en los desarrollos jurídicos en Colombia del tema puede consultarse el Alexeio Julio (2000)

Pérez Luño resume con precisión en que consiste, así como los espinosos temas referentes al uso de unos derechos que se fundamentaron para proteger frente a las actividades particulares que los amenacen:

“Un problema más arduo es el que se refiere a la *titularidad* de los derechos sociales y su eficacia frente a terceros. Ya que, en muchas ocasiones, el Estado no realiza directamente las obligaciones que se derivan de estos derechos (...) El problema ha sido abordado con especial atención por la doctrina y la jurisprudencia alemana en relación con la denominada *Driuwirkung der Grundrechte* (eficacia frente a terceros de los derechos fundamentales). Se trata, en suma, de la aplicación de los derechos fundamentales no sólo en las relaciones entre el Estado y los ciudadanos, sino también en las relaciones entre personas privadas” (Pérez Luño, 2005:94-95)

La eficacia frente a terceros de los derechos fundamentales proyecta una extensión de la dimensión objetiva⁹⁵ de los derechos fundamentales (Julio, 2000:20), como normas de estricto cumplimiento, casi que de orden público, y el rasgo más importante: universalmente válidas. Esta nueva teoría borra por completo la separación entre el Derecho Privado y el Derecho Público o más específicamente el Derecho Constitucional; el efecto de la fuerza vinculante de la Constitución se aprecia en su mayor esplendor. De acuerdo con esto tres son los factores de importancia para comprender porque se proyectan los derechos fundamentales frente a un sujeto no-estatal (Julio, 2000:66 y ss.)⁹⁶:

- Esfera objetiva⁹⁷: Normas que pueden aplicarse directamente, sin esperar su desarrollo, por lo que se transforman en imperativas, de cumplimiento inmediato y desarrollo

⁹⁵Los derechos fundamentales emanados de la Constitución, imponen un mandato de actuación o de optimización, lo que implica el cumplimiento en la mayor medida posible para las autoridades y los particulares.

⁹⁶Para Néstor Osuna (1998:253) son: suprallegalidad constitucional, rigidez, vinculación general e invocabilidad directa.

⁹⁷ En este sentido confirma Alexei Julio(2000:66) que la teoría objetiva concibe los derechos fundamentales con una dimensión que los pone “(...) como valores supremos que rigen para todo el ordenamiento jurídico, también informan las relaciones recíprocas entre particulares, y limitan la autonomía privada, al mismo tiempo que fungen como mandatos de actuación y deberes de protección para el Estado”

posterior, por ser mandatos de optimización, que exigen su cumplimiento en la mayor medida posible.

- Efecto de irradiación⁹⁸: Los derechos fundamentales ejercen una influencia axiológica en la manera de entender todos los ámbitos y normas del ordenamiento jurídico por virtud de la supremacía de la Constitución en el ordenamiento jurídico, a partir de su dimensión objetiva reconocida. [Q]ue tienen valor para todos los ámbitos del derecho” y “(...) este efecto no se limita en modo alguno a un derecho determinado, porque es propio “fundamentalmente” a todos ellos, sin consideración a su formulación particular, la que solamente puede indicar el grado de intensidad”(Julio,2000:63 y 72-77)
- Deber de protección⁹⁹: En virtud del principio de *supremacía de la Constitución*, del principio *pro homine* y del principio de la *dignidad humana*, se transforman en derechos inherentes al ser humano¹⁰⁰, cuya guarda, por orden constitucional y recientemente por el control de convencionalidad¹⁰¹, puede exigirlos de manera directa y al mismo tiempo establece la obligación de las autoridades por asegurar su eficacia en el ordenamiento jurídico: expidiendo normas, vigilando, inspeccionando las actividades particulares(Julio,2000:74-83)

En el ordenamiento jurídico colombiano se reconoce la eficacia directa¹⁰² de los derechos fundamentales entre particulares a través de dos normas: la norma constitucional del

⁹⁸Sobre este efecto Smend (1985:229 cit. por Alexei (2000:63) dice que se debe a que establecen fines específicos a cada ámbito del derecho público y privado, los cuales pasan a ser integrados por el Derecho Constitucional.

⁹⁹Al respecto dice Alexei Julio (2000:66): “En efecto, la caracterización de la constitución como “ley superior”, con una fuera normativa propia, dentro de la que juegan un papel determinante los derechos fundamentales, que gozan a su vez de una posición reforzada (pues cuentan con una protección, ante eventuales modificaciones, superior a la de las restantes normas constitucionales y vinculan al mismo legislador) (...)”

¹⁰⁰Según el profesor Alexei Julio Estado “(...) el bien jurídico iusfundamentalmente protegido hace parte de la personalidad de su titular, y como tal tiene una pretensión de validez universal, frente a cualquier amenaza o lesión, y no sólo ante aquéllas que provengan de las autoridades estatales”

¹⁰¹Para ver más de este tema Quinche. Manuel (2015). El Control de convencionalidad. Bogotá: Temis

¹⁰²A nivel doctrinal la otra tesis afirma la eficacia indirecta de los derechos fundamentales, que afirma la necesidad de desarrollarlos a través del desarrollo legal con cláusulas generales y conceptos adaptados a las necesidades del derecho privado. Alexei Julio (2000:111) resume la tesis afirmando que “(...) las cláusulas y conceptos generales de derecho privado, como instrumentos normativos idóneos para ser “colmados”, por decirlo de alguna manera con el contenido de los valores

artículo 86 y la norma con fuerza de ley del decreto 2591 de 1991 en su artículo 42. En este último destaca la procedencia de la acción de tutela para la protección del habeas data en el numeral 6. Más adelante se tratará la acción de tutela como herramienta jurídica de protección del habeas data.

La Corte Constitucional¹⁰³ colombiana afirma que los datos personales deben administrarse de tal manera que se respeten los derechos fundamentales, entre esos se incluye el habeas data. Dada la proyección social de la actividad del individuo que tienen en su actividad gubernamental, social, económica, su ámbito de aplicación se extiende más allá de las relaciones individuo-estado, el habeas data deja de ser un derecho de defensa frente al estado para serlo *erga omnes*, es decir, exigible su eficacia a toda la sociedad.

El derecho fundamental a la protección de datos personales de manera radiante confirma la validez de la teoría de la eficacia hacia terceros de los derechos fundamentales, porque actualmente el poder informático es mayormente ejercido por grandes empresas que fundamentan su modelo de negocio en recopilar, conocer, comprender y tomar decisiones de datos personales facilitados a diario por millones de personas en el mundo. Afirmar que esta teoría no tiene piso jurídico, dejaría ante una evidente falta de tutela jurídica del individuo frente al nuevo leviatán: las compañías de internet y en general las multinacionales de base informáticas¹⁰⁴.

típicos de los derechos fundamentales, los que de este modo encuentran el vehículo de su operatividad en el campo del derecho privado”

¹⁰³ “Así las cosas, en virtud de la aplicación del principio *pro homine*, propio de la interpretación de las normas de la Carta Política, la administración de datos personales deberán, en todo caso, subordinarse a la eficacia de los derechos fundamentales del individuo. Así mismo, los principios deben entenderse de manera armónica, coordinada y sistemática, respetando en todo caso los contenidos básicos del derecho fundamental al habeas data.” (Sentencia C-748 de 2011)

¹⁰⁴ Aquellas empresas cuyos modelos de negocio necesitan de la recolección y análisis de información. Por ejemplo Facebook, WhatsApp, Instagram, Twitter, Google, Microsoft.

Herramientas jurídicas para la protección de datos personales en Colombia

“[P]or el bien de la dignidad
De las personas, hay que proteger
El pleno ámbito privado de vulneración
Por las cada vez más sutiles
Posibilidades técnicas”
Ernesto Benda

Dignidad Humana y derechos de la personalidad

La protección de datos personales a través de un adecuado marco jurídico que exprese el cumplimiento de los derechos constitucionales y cree las herramientas institucionales, hace parte del requisito de efectividad de los derechos fundamentales que se impone al estado social de derecho fijado por la Constitución colombiana vigente.¹⁰⁵

La Corte Constitucional lo confirma en sentencia T-307 de 1999: “El Estado debe diseñar mecanismos de protección que aseguren la participación de las personas en el proceso de acopio así como el ejercicio pleno de los derechos a la corrección o actualización de las informaciones que les conciernan.”

En 1992 el máximo tribunal de lo constitucional afirmó la necesidad de una reglamentación procesal que supere los derechos de petición y la acción de tutela, al ser instrumentos poco adecuados: “La Corte Constitucional ha insistido en **la necesidad de una reglamentación general y coercitiva que garantice el ejercicio pleno de los derechos que se derivan del habeas data**. Sin embargo, ello no ha ocurrido. En consecuencia, las personas han debido recurrir a mecanismos como el derecho fundamental de petición o la acción de tutela para impedir eventuales vulneraciones a su derecho a la autodeterminación informativa. No obstante, estos mecanismos resultan algunas veces insuficientes para la garantía plena,

¹⁰⁵En esto concuerda el Tribunal Constitucional Federal de Alemania (sentencia de 15 de diciembre de 1983) al decir que “(...) para asegurar el derecho a la autodeterminación informativa hacen falta precauciones complementarias de derecho procesal (...)” que se refieran a la recogida de datos, lo cual modernamente puede referirse a los principios para el tratamiento de ellos y a la “organización”, en cuanto a una estructura robusta que sea confiable al ciudadano.

También la Corte Constitucional colombiana ha afirmado que “(...) tales herramientas pueden ser tanto de naturaleza judicial como administrativa, es decir, el literal a) hace referencia (i) tanto a acciones o recursos que permiten reclamar la satisfacción de un derecho ante un juez y que implican la existencia de un proceso, (ii) como a mecanismos administrativos tales como órganos de vigilancia y control y procesos administrativos dirigidos a resolver controversias relacionadas con la realización de los derechos fundamentales.” (Sentencia C-748 de 2011)

pronta y efectiva de los derechos comprometidos en el proceso informático. En efecto, no sólo se trata de garantías ex post, que no establecen ab initio reglas claras para todas las partes comprometidas en este proceso, sino que muchas veces no tienen el alcance técnico que se requiere para lograr la verdadera protección de todos los bienes e intereses que se encuentran en juego.” (Negrilla fuera de texto)

Los mecanismos que protegen los derechos principales y otros relacionados con el habeas data son de variada índole¹⁰⁶. Se encuentran la tutela judicial como: i) la acción de tutela para prevenir una vulneración inminente, en caso de no ser este el criterio puede ejercerse; ii) la acción ordinaria de responsabilidad civil contractual o extracontractual; iii) la acción ejecutiva para que cumpla el contrato, en el caso de normas corporativas vinculantes y las políticas de tratamiento de la información; iv) acción penal cuando se tipifiquen cualquiera de las conductas que afectan indirectamente al debido tratamiento de datos personales (como los artículos 269B y 269C) o directamente (como en los artículos 269D, 269F y 269G)

Ahora dentro de la tutela administrativa puede quejarse ante la Autoridad Nacional de Protección de Datos Personales, que en Colombia es la Superintendencia de Industria y Comercio, para ello debe agotar el requisito de procedibilidad que inicia con el derecho de petición ante el responsable del tratamiento del dato personal con cualquiera de los denominados derechos ARCO que sea correspondiente a la información, que la ley 1581 de 2012 denomina “reclamo”. Cuando la persona jurídica o natural responsable no entregue una respuesta satisfactoria, el ordenamiento jurídico prevé la habilitación de la interposición de la queja ante la Superintendencia de Industria y Comercio, en su oficina Delegada para la Protección de Datos Personales, contra el encargado o responsable del tratamiento que no realiza el cumplimiento de los derechos ARCO y así garantizar el derecho a la intimidad.

¹⁰⁶“Este derecho como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben pender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones.” (Sentencia C-748 de 2011 MP Jorge Pretelt Chaljub MP Jorge Pretelt Chaljub)

Vulneración del derecho de Habeas Data

La jurisprudencia constitucional ha considerado dos ocasiones en las cuales se viola el derecho al Habeas Data: i. cuando no pueden ejercerse cualquiera de los derechos asociados que se denominan ARCARS¹⁰⁷ y ii. Cuando se presenta un incumplimiento a cualquiera de los principios rectores para la administración y tratamiento de datos personales (PRATDP)¹⁰⁸.

a) Negación del ejercicio de los derechos ARCARS

El responsable y encargado tienen en común el deber de fijar procedimientos para que las personas puedan acceder a sus datos personales y ejercer los derechos relacionados con ellos: acceso, rectificación, cancelación y oposición, llamados derechos ARCO. Cuando no se tienen establecidos los procedimientos o se incumplen flagrantemente, queda habilitada la tutela como herramienta jurídica de protección transitoria o la queja administrativa ante la Superintendencia de Industria y Comercio para que inicie la investigación administrativa pertinente.

Adicionalmente si la vulneración de cualquier derecho ARCARS tiene consecuencias de daño patrimonial o moral pueden iniciarse acciones de responsabilidad civil por incumplimiento del contrato, en el marco de una Política de Tratamiento de Datos Personales propiamente como contrato o incorporada como cláusula o cláusulas en un contrato, o de manera extracontractual a través de dos vías: como reparación en un proceso penal cuando se presenten algunos de los delitos establecidos en la ley 1273 de 2009 o de manera independiente en un proceso ordinario civil..

¹⁰⁷En sentencia C-748 de 2011 se sistematiza así: “De la misma forma, en la Sentencia T-176 de 1995 la Corporación dijo que la falta de consentimiento se traduce en una vulneración de los derechos al habeas data: “para que exista una vulneración del derecho al habeas data, 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.”

¹⁰⁸Estos principios se encuentran analizados en la sentencia T-729 de 2000.

Esta negación es de tal importancia para la Corte Constitucional que en sentencia T-307 de 1999, fallo a favor de la accionante la protección de su derecho fundamental al habeas data invocado porque la división de sistemas encargada del SISBEN en el municipio de Ibagué, no tenía un mecanismo claro para ejercer los derechos ARCO que permitiera administrar sus datos personales de manera clara, eficaz y específica. Al respecto transcribimos la idea:

“En efecto, las personas que habitan en la ciudad de Ibagué y que son beneficiarias – potenciales o actuales – de los programas sociales cuya focalización se realiza mediante el mencionado Sistema, **no tienen mecanismos específicos, claros y eficaces** para enterarse de los datos personales que les conciernen y que reposan en el respectivo banco de datos. Tampoco existen **instrumentos formales y eficaces** a través de los cuales puedan solicitar el ingreso de sus datos al sistema o exigir que una información errónea, inexacta, incompleta o desactualizada, sea corregida o excluida del banco de datos. Por último, es evidente que **no tienen la capacidad de controlar que la información por ellos suministrada se use exclusivamente para los fines** para los cuales fue creado este mecanismo de focalización del gasto.”

- b) Incumplimiento a los principios para la administración y tratamiento de datos personales (PRATDP)

Los encargados de realizar el tratamiento de datos personales deben cumplir con principios constitucionales cuando realizan la actividad, para evitar la vulneración de derechos a la intimidad, al buen nombre, a la honra, a la imagen, al olvido. La sentencia de la Corte Constitucional que sistematiza todos estos principios es la T-729 de 2000 y los vuelve a analizar en la sentencia de C-748 de 2011 que revisa la constitucionalidad del proyecto de ley que sería luego la Ley Estatutaria de Protección de Datos Personales (LEPDP).

La sentencia T-279 de 2000 la Corte comenta algunos de los principios iniciales:

- i) Principio del consentimiento libre, previo y expreso, lo que significa que debe informársele al titular las condiciones bajo las cuales se recolectará, almacenará y usará la información, la relación jurídica bajo la cual se realiza, la finalidad de la

información solicitada para que la persona comprenda finalmente la magnitud de la autorización que está realizando.

- ii) El segundo principio se trata acerca de la necesidad de pedir los datos que sean necesarios para la realización del fin estipulado bien sea en la relación jurídica marco o en lo que dio origen a la entrega y el consentimiento, de esta manera no se pide un consentimiento tan amplio que haga nulo el efectivo control de los datos *a posteriori* entregados.
- iii) El tercer principio se trata acerca de la realidad del dato personal o su veracidad, de esta manera se evitan que se guarden datos erróneos o falsos, los cuales terminan afectando el buen nombre o la honra o el honor de la persona.
- iv) El cuarto principio mira muy acerca de la integridad del dato, es decir, de que refleje lo más claro y detallado posible a realidad, limitado por el siguiente principio y por el del consentimiento informado.
- v) Principio de finalidad se establece para que la recolección del dato personal obedezca a una fin constitucional legítimo, claro, suficiente y previo pues es requisito para que el titular del dato personal dé el consentimiento.
- vi) El principio de utilidad establece que los datos personales recolectados deben usarse para la finalidad explicada al titular del dato.
- vii) El principio de la circulación restringida proviene del derecho de la intimidad, recuerda un poco a ese espacio reservado que nadie más puede entrar, sólo quien tenga autorización. Precisamente por esta razón los datos no pueden comunicarse a otras personas, para lo cual deberá contar con la autorización previa en virtud del principio del consentimiento.

- viii) El principio de incorporación se justifica cuando se beneficie (acceso a servicios, derechos o subsidios) el titular por tener incorporado un dato personal en alguna base de datos.
- ix) El principio de caducidad se aduce para evitar que datos negativos se conserven indefinidamente y den una afectación a la reputación de la persona cuando no existen causales para ello.

Herramientas técnicas de protección de datos personales

El tratamiento de los datos personales por medio de las nuevas tecnologías pueden afectar los derechos fundamentales. La manera en que muchos responsables y encargados de realizar el tratamiento de datos personales pueden impedirlo es a través de la decisión de implementar medidas técnicas para realizar el tratamiento que permiten ocultar la identidad de la persona o limitar la pedida de información a datos específicos. Como medida técnica para ocultar la identidad o difuminarla se tiene *la seudonimización, la encriptación, el enciframiento, la anonimización*. (cfr. CE, 2007:17 y ss.)

La utilización de seudónimos permite recopilar bastante información acerca de una persona, sin que en conjunto pueda identificarse rápidamente; es un procedimiento por medio del cual se selecciona aleatoriamente un “nombre falso”. Un buen ejemplo lo constituyen la forma de navegación privada que se encuentran en varios navegadores web que evitan asociar el historial de navegación por sitios web con una dirección IP específica o con los hábitos de navegación previamente almacenados acerca de ese dispositivo.

El enciframiento es un procedimiento por medio del cual se convierten los datos en un código determinado y una clave para acceder a los datos, sin esa clave es imposible acceder a la identidad real y determinar a quién pertenecen los datos. El código es un algoritmo de encriptación/descenciptación que de acuerdo a la llave que le presente permitirá su acceso con el desciframiento o la bloqueará, “(...) lo que permite minimizar el riesgo de que una persona

no autorizada pueda interceptar el texto cifrado y obtener el texto original que se envió” (Peña, 2007:175); el más usado es el *Secure Sockets Layer* para comunicaciones en internet y para almacenamiento de la información se usan los *backup* o respaldos periódicos en discos duros externos o servidores espejo, entre otras tecnologías que existen en el mercado.

También algunos programas de encriptación como el *Pretty Good Privacy PGP* de Philip Zimmermann son ejemplos de software destinados a asegurar la confidencialidad en la transmisión de informaciones lícitas. (Pérez Luño, 2006:95)

La anonimización consiste en separar de la información los datos que puedan identificar a una persona específica, de esta manera ya no es posible realizar un análisis de pertenencia a esa persona.

El fin de estas herramientas técnicas es asegurar la privacidad de la información personal, el acceso por las personas consentidas y al mismo tiempo el control del tratamiento de la información para las finalidades permitidas

Herramientas jurídicas: tutela judicial y tutela administrativa

Los derechos subjetivos tienen la vocación de generar efectos jurídicos que satisfacen un interés jurídico protegido. Cuando en muchas ocasiones se presentan impedimentos externos que no dejan gozar plenamente de sus derechos, las personas afectadas deben tener alguna posibilidad de hacerlos cumplir; es inherente a ellos su cumplimiento para garantizar la seguridad jurídica y la convivencia, ciertamente en los términos Lockeanos es garantizar la existencia de la sociedad civil.

La Corte Constitucional tiene la posición que las herramientas jurídicas para la protección de derechos fundamentales o la garantía de su efectividad son de diversa naturaleza, esto lo decide el legislador en la misma ley estatutaria o en ley estatutaria aparte. “Ahora bien, tales herramientas pueden ser tanto de naturaleza judicial como administrativa, es decir, el literal a) hace referencia (i) tanto a acciones o recursos que permiten reclamar la

satisfacción de un derecho ante un juez y que implican la existencia de un proceso, (ii) como a mecanismos administrativos tales como órganos de vigilancia y control y procesos administrativos dirigidos a resolver controversias relacionadas con la realización de los derechos fundamentales.”

El Estado entra en la escena, estableciendo los instrumentos válidos para hacer cumplir los derechos, aún contra lo que se oponga, siempre que venga de un hecho provocado por las personas¹⁰⁹, se llaman acciones procesales. “La presencia de condiciones anómalas o irregulares que impiden el goce tranquilo de los derechos o estados, engendra la teoría de las acciones civiles” (Valencia Zea, 2006:311) El Estado es el encargado de proteger el ordenamiento jurídico porque es el portador de la jurisdicción, que tiene el fin primordial de garantizar la efectividad del ordenamiento jurídico (Constitución, leyes, decretos, etc.)

El profesor Arturo Valencia Zea (2006:314) menciona las circunstancias que impiden el ejercicio perfecto de los derechos: i) cuando el derecho es violado o desconocido por otro, ii) cuando el derecho no es reconocido como existente, iii) cuando el derecho tiene riesgo de no generar efectos jurídicos por prescripción o nulidad o inexistencia iv) cuando se busca que se transforme en otro derecho, v) cuando el derecho no es realizado por el obligado voluntariamente.

La teoría de las acciones civiles permite comprender que a las personas se le ha otorgado un derecho subjetivo de obtener una protección de sus otros derechos, quien está a cargo es el Estado (Valencia Zea, 2006:312). En Colombia es elevado a derecho fundamental en el ordenamiento constitucional, se puede encontrar en el artículo 229. El estado ejerce soberanamente la administración de justicia, a través de la cual cumple esa obligación de proteger los derechos, esto se denomina jurisdicción, definida por Couture¹¹⁰ como:

¹⁰⁹Cabe hacer esta declaración pues no debe olvidarse que las obligaciones y los derechos que generan se dan entre personas naturales y jurídicas.

¹¹⁰Couture, Eduardo (1980). *Vocabulario Jurídico.*, Buenos Aires: Depalma, p. 369 y en el mismo sentido Devis Echandia, Hernando. (1966) *Nociones generales de derecho procesal civil.* Bogotá: Aguilar, p. 70.

“[L]a función pública realizada por órgano competente del Estado, con las formas requeridas por ley, en virtud del cual, por acto de juicio y la participación de sujetos procesales, se determina el derecho de partes, con el objeto de dirimir sus conflictos de relevancia jurídica, mediante decisiones con autoridad de cosa juzgada, eventualmente factibles de ejecución. “

Adicionalmente se ha creado una institucionalidad estatal encargada de vigilar y controlar el cumplimiento de las normas sobre habeas data, en ejercicio de la facultad asignada al presidente de la República en el artículo 189-10 de la Constitución. Para ello se han habilitado una modalidad especial del derecho de petición que denomina queja ante la Superintendencia de Industria y Comercio (SIC) y se le adicionaron facultades a la SIC para iniciar investigaciones bajo el procedimiento administrativo sancionatorio que regula la ley 1437 de 2011.

Tutela judicial

Se encuentran la tutela judicial como: a) la acción de tutela para prevenir una vulneración inminente o en tanto los otros mecanismos le resten efectividad al derecho al demorarse mucho; b) la acción ordinaria de responsabilidad civil contractual o extracontractual; c) la acción ejecutiva para que cumpla el contrato, en el caso de normas corporativas vinculantes; d) acción penal cuando se tipifiquen cualquiera de las conductas que afectan indirectamente al debido tratamiento de datos personales (como los artículos 269B y 269C) o directamente (como en los artículos 269D, 269F y 269G)

a) Acción de tutela

En el artículo 86 de la Constitución Política de Colombia de 1991 se consagra la acción de tutela como mecanismo para proteger la efectividad de los derechos fundamentales de la

Constitución y siempre que no exista otro medio adecuado de protección inmediata de los derechos fundamentales.¹¹¹

La Acción de Tutela es un mecanismo constitucional para garantizar que se conserve el nuevo enfoque jurídico centrado en el ser humano y su persona, de esta manera se obtenga la permeabilidad activa y constante de la filosofía jurídica de la Constitución en todo el ordenamiento jurídico y en todas las situaciones de hecho que se presenten a diario.

Es pertinente a la acción de tutela explicar dos aspectos para comprender la importancia que ha tenido en el desarrollo jurisprudencial del derecho al habeas data: i) acción de tutela contra particulares para proteger el habeas data y ii) La indemnización de perjuicios causados por la violación del derecho.

i) Acción de tutela para proteger el habeas data

Al final del artículo 86 de la Constitución Política de Colombia queda la obligación en la ley sobre la regulación de la acción de tutela contra los particulares bajo tres hipótesis: a. Estén encargados de la prestación de un servicio público; b. Realicen conductas que afectan grave y directamente el interés colectivo y c.- Respecto de quienes el solicitante se halle en estado de subordinación e indefensión.¹¹² Posteriormente en el decreto-ley 2591 de 1991 se desarrolla los supuestos de hecho necesarios para que proceda la acción de tutela contra particulares, respecto de los cuales la Corte Constitucional considera que es una lista taxativa (sentencia T-303 de 1993 MP Hernando Herrera Vergara) y frente a lo cual hay un estudio profundo sobre el tema del profesor Alexei Julio Estrada llamado “*La Eficacia de los derechos fundamentales entre particulares*”. En esta lista destaca el numeral 6 que dice:

¹¹¹Sentencia T-414 de 1992 MP Ciro Angarita Baron afirma: “En otros términos, en virtud de lo dispuesto por la carta del 91, no hay duda que “el otro medio de defensa judicial” a disposición de la persona que reclama ante los jueces la protección de sus derechos fundamentales ha de tener una efectividad igual o superior a la de la acción de tutela para lograr efectiva y concretamente que la protección sea inmediata. No basta, pues, con la existencia en abstracto de otro medio de defensa judicial si su eficacia es inferior a la de la acción de tutela.”

¹¹²Artículo 86. (...)La ley establecerá los casos en los que la acción de tutela procede contra particulares encargados de la prestación de un servicio público o cuya conducta afecte grave y directamente el interés colectivo, o respecto de quienes el solicitante se halle en estado de subordinación o indefensión.

Artículo 42. Procedencia. La acción de tutela procederá contra acciones u omisiones de particulares en los siguientes casos:

(...)

6. Cuando la entidad privada sea aquella contra quien se hubiere hecho la solicitud en ejercicio del habeas data, de conformidad con lo establecido en el artículo 15 de la Constitución.

La regulación en el artículo 42 del decreto-ley 2591 de 1991 se fundamenta en el derecho reconocido en la segunda parte del artículo 15 Constitucional como un derecho a “(...) conocer, actualizar y rectificar todas las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas”. El contenido de este derecho será analizado posteriormente en su objeto constitucionalmente protegido¹¹³, por ahora se puede afirmar que los efectos de este derecho, cuando se inicia una acción de tutela, es que permite el control de la información personal.

Las nuevas tecnologías se convierten en un aliado potencial del hombre, quien las utiliza en su vida cotidiana para facilitarse algunas tareas, pero ese uso provechoso para las personas puede hacerse a costa de los derechos de otros, lo hemos visto en la sección 1.1 acerca del origen del derecho al Habeas Data en el llamado poder informático, que comenzó a afectar las esferas de libertad de las personas, quienes vieron como cedían sus derechos ante el potencial económico de aplicar la tecnología al tratamiento automatizado de los datos de personas recogidos en bases de datos. “Por tanto, en Colombia la actividad económica no puede desarrollarse hoy en abierto contraste con los valores fundamentales y las exigencias propias de la libertad humana. Ella prevalece sobre toda pretensión desmesurada de servir los intereses de la productividad y la eficiencia.”(Sentencia T-414/1992 MP. Ciro Angarita Baron).

Ahora para que sea procedente la acción de tutela, en la protección del derecho al debido tratamiento de datos personales o habeas data, se requiere que haya existido una posible renuencia del encargado de la base de datos a cumplir cualquiera de los derechos ARCO antes

¹¹³Ver infra página 285

mencionados bien sea a partir de una contestación a la solicitud radicada o con la omisión de la respuesta al cumplimiento de algunos de los principios de administración o tratamiento de datos personales; o también se esté ante un daño futuro inminente a otros derechos fundamentales como el buen nombre, la imagen y la intimidad, lo cual coloca en estado de indefensión en estos derechos al titular del dato personal. De esta manera se cumple lo enunciado en la parte inicial del artículo 86 acerca de estar los derechos constitucionales amenazados o haber sido vulnerados por cualquier autoridad pública o privada (art. 42 decreto-ley 2591 de 1991).

ii) La indemnización de perjuicios causados por la violación del derecho

Los particulares en ejercicio de las actividades de recolección y tratamiento de datos personales están profundamente vinculados al cumplimiento de los principios establecidos por la Corte Constitucional y volcados al artículo 4 de la ley 1581 de 2012, por otro lado también están obligados a garantizar el ejercicio de los derechos de habeas data bien como responsable del tratamiento de datos personales (literal a artículo 17 de la LEPDP) y/o como encargado del tratamiento (literal a artículo 18 de la LEPDP).

El tratamiento de datos personales es una actividad reglamentada por la jurisprudencia constitucional y la LEPDP, se permite no sólo si hay un apego formal a estas leyes y jurisprudencia sino de manera material sin que se vulneren los derechos constitucionales reconocidos, pues mal podría permitirse una nueva forma de tratamiento no regulado por la ley o analizado por la jurisprudencia que violentara los derechos a la intimidad, el buen nombre o el habeas data, entre otros. Al respecto la Corte ha analizado esta situación concluyendo que al ser los datos un reflejo de “(...) la personalidad del individuo (honestidad, honorabilidad, confiabilidad, etc.), exige de las entidades privadas y públicas que manejan estas centrales y bancos de datos un comportamiento caracterizado por el máximo grado de diligencia y razonabilidad.” (Sentencia T-303 de 1993 MP Hernando Herrera Vergara)

En virtud de lo anterior, cuando se presenten tratamientos automatizados o mecánicos de datos personales que generen perjuicios habrá que examinar el perjuicio moral y económico generado a la persona. Cabe recordar que esto es reconocido tanto en el código civil colombiano (artículos 1613¹¹⁴ y 2341¹¹⁵) como a nivel constitucional con fundamento principal en la afectación de la personalidad jurídica y los derechos integrantes que ocurre¹¹⁶ y en la doctrina como el daño moral y el daño patrimonial, este último dividido en daño emergente y lucro cesante. La cuantificación y cualificación del daño dependerá de los aspectos probatorios acerca de las consecuencias que generó la conducta desplegada por el administrador responsable o encargado de la base de datos.

b) Acción de responsabilidad civil por indebido tratamiento de datos personales

La reacción jurídica frente a la vulneración del Habeas Data es de dos clases: la investigación administrativa o penal para sancionar la conducta de administrador de la base de datos (encargado o responsable del tratamiento) y el reconocimiento al titular del dato vulnerado de un derecho a la reparación. Estamos en el primer caso ante el derecho sancionatorio¹¹⁷ y en el segundo caso frente a una responsabilidad civil, porque “(...) engloba todos los comportamientos ilícitos que por generar daño a terceros hacen recaer en cabeza de quien lo causó, la obligación de indemnizar” (Tamayo, 2007:8) como bien lo define Tamayo (2007:8).

A continuación se enfocará en el segundo supuesto: la responsabilidad civil por la vulneración del derecho al debido tratamiento de datos personales, aclarando que no existen normas específicas para el Habeas Data, por lo cual nos remitiremos a los aspectos generales de la doctrina y la ley que sean pertinentes para el tema. El primero supuesto se tratará en la

¹¹⁴ARTICULO 1613. <INDEMNIZACIÓN DE PERJUICIOS> La indemnización de perjuicios comprende el daño emergente y lucro cesante, ya provenga de no haberse cumplido la obligación, o de haberse cumplido imperfectamente, o de haberse retardado el cumplimiento.

¹¹⁵ARTICULO 2341. RESPONSABILIDAD EXTRA CONTRACTUAL. El que ha cometido un delito o culpa, que ha inferido daño a otro, es obligado a la indemnización, sin perjuicio de la pena principal que la ley imponga por la culpa o el delito cometido.

¹¹⁶Ver supra “Dignidad humana y los derechos de la personalidad”

¹¹⁷Este será tocado en la acción penal, competencia de los jueces penales y en el procedimiento administrativo sancionatorio a cargo de la Superintendencia de Industria y Comercio

sección de la Tutela administrativa, ya que es un asunto cuya competencia administrativa fue asignada a la Superintendencia de Industria y Comercio.

i) Contenido de la responsabilidad civil por indebido tratamiento de datos personales

El ordenamiento jurídico colombiano reconoce el derecho de indemnizar según la fuente de las obligaciones (Art.1494 y Art.2341 del Código Civil) que lo genere: contractual o extracontractual (cuasidelito o delito)¹¹⁸. En el primer caso, la fuente que lo genera son las obligaciones incumplidas por una de las partes en el contrato acordado, por expresa autorización del artículo 1495 del Código Civil que le reconoce la fuerza vinculante. En el segundo caso, se cuenta con el enunciado del artículo 2341 del Código Civil que obliga reparar el daño causado por una o varias personas a otra mediante dolo o culpa.

Ante un indebido tratamiento de datos personales se producirán diversas afectaciones, dependiendo de si toca aspectos patrimoniales o no patrimoniales de la persona, así como también si se dio dentro de una obligación contractual o por efecto de un tercero con quien no se tiene relación jurídica pero accedió ilícitamente a los datos personales. La acción de responsabilidad civil dependerá del tipo de agresor causante del hecho productor del daño: si es una persona de derecho privado vale esta misma acción, pero si es una de derecho público la situación pasa a ser procedente con el medio de control de la reparación directa.

La responsabilidad civil será contractual¹¹⁹, cuando el interés “sacrificado” del sujeto pasivo, es el incumplimiento de los lineamientos de tratamiento de la información personal que se incorporan como cláusulas de un contrato o en virtud de que sea un contrato autónomo denominado “Políticas de tratamiento de la información”; habrá responsabilidad

¹¹⁸La fuente de las obligaciones extracontractual son el delito y el cuasidelito que se engloban en la noción de hechos ilícitos, “el hecho jurídico voluntario ilícito (...)”(Valencia Zea,2006:297)

¹¹⁹ La *responsabilidad contractual* se origina en la violación del artículo 1602 del Código Civil que afirma la obligatoriedad del cumplimiento del acuerdo o contrato entre las partes, por ello cuando se incumple y genera una frustración a la expectativa legítima de cumplimiento, provocando una alteración del derecho ya adquirido preexistente que se ve “borrado” o se torna imposible de ejecutar, ocurre lo que menciona Alessandri(1943:42) y “(...) es la que se origina en la violación de un contrato (continuación nota 119) o convención; consiste en la obligación de indemnizar al acreedor el perjuicio que le causa el incumplimiento del contrato o su cumplimiento tardío.”

extracontractual¹²⁰ cuando la irrupción en el ámbito privado haya sido sin la autorización para realizar el tratamiento con una finalidad clara, que es el generador del vínculo jurídico. Junto al indebido tratamiento de datos personales pueden incluirse afectaciones a la intimidad, el buen nombre y la honra.

El régimen de responsabilidad civil que establezca el ordenamiento jurídico incide profundamente en el aspecto probatorio de los hechos imputables (Tamayo Jaramillo, 2007:32). En efecto si aplica un régimen subjetivo de responsabilidad deberá probarse que el sujeto cometió el hecho, en qué medida es responsable (con dolo o culpa); cuando aplique un régimen objetivo de responsabilidad simplemente basta con probar que el sujeto cometió el hecho y que evidentemente este afectó a la persona¹²¹

El ordenamiento jurídico colombiana ha sido adaptado a las nuevas circunstancias económicas y sociales por parte de los jueces, de ello no se excluye el régimen de responsabilidad civil. Esta afirmación es adecuada debido a que se ha pasado de un régimen predominantemente de culpa a otro objetivo, esto bien lo afirma Mantilla Espinosa (2007:134-136) fundamentado en la interpretación que ha hecho la jurisprudencia de los artículos 1603¹²² y 2356¹²³ del código civil colombiano. Con frecuencia, para ayudar en la imputación de responsabilidad, en materia contractual se aplica la distinción teórica de obligaciones de

¹²⁰ La *responsabilidad extracontractual* (delictual o cuasidelictual) proviene de un hecho ilícito civil producido por una persona, con intención o no, que lesiona a otra; en este tipo de responsabilidad no existe obligación preexistente y se basa en el principio genérico de que toda persona responderá por los daños causados, que fija el artículo 2343 del Código Civil colombiano. Alessandri (1943:43) lo resume en que el daño es el mismo generador de la obligación de reparar. Este tipo de responsabilidad cuando se funda en el dolo o culpa de la persona es objetiva; cuando se funda en el riesgo latente de la actividad, es objetiva.

¹²¹ Al respecto sobre la explicación de estos regímenes de responsabilidad civil nos amplia Mantilla Espinosa (2007:134): “Normalmente, se entiende que los regímenes subjetivos de responsabilidad son aquellos cuyas normas exigen que el sujeto normativo haya actuado con culpa, a fin de obligarlo a reparar el daño, mientras que las normas de los regímenes objetivos no establecen ningún juicio de valor como condición de sus supuestos de hecho.”

¹²² ARTICULO 1603. EJECUCION DE BUENA FE. Los contratos deben ejecutarse de buena fe, y por consiguiente obligan no solo a lo que en ellos se expresa, sino a todas las cosas que emanan precisamente de la naturaleza de la obligación, o que por ley pertenecen a ella.

¹²³ ARTICULO 2356. RESPONSABILIDAD POR MALICIA O NEGLIGENCIA. Por regla general todo daño que pueda imputarse a malicia o negligencia de otra persona, debe ser reparado por ésta.

medio y de resultado¹²⁴, en materia extracontractual se acude a la teoría de las actividades peligrosas.

Puede apreciarse que el régimen de responsabilidad civil mejor aplicable por una violación del tratamiento adecuado de datos personales en materia extracontractual y contractual es objetivo, en el primero caso atendiendo a que la actividad entraña profundos riesgos para el titular del dato personal y en el segundo caso a que la obligación es de resultado puesto en esta basta con probar el incumplimiento de la finalidad para ello consentida, teniendo en cuenta que esta se fija como uno de los principios inherentes a la autorización para realizar el tratamiento de los datos del titular. Se acude para ello a la interpretación de la jurisprudencia constitucional¹²⁵ y la LEPDP.¹²⁶ El régimen de responsabilidad civil es objetivo porque los responsables del tratamiento deben realizarlo según los principios rectores de la LEPDP, se excluye el hecho de que existe culpa al respecto porque la violación de cualquiera de estos genera un daño pues tiene el deber de cuidado ante el riesgo que conlleva la actividad. En efecto dados los riesgos potenciales para las personas, en su intimidad y en su patrimonio, con la sola divulgación de la información o el acceso no autorizado o el uso para fines no autorizados son hechos perjudiciales *per se*, cuando no se tienen implementadas por orden todas las medidas administrativas y técnicas que cumplan con los principios rectores por orden de la misma LEPDP.

Otro argumento a favor de un régimen objetivo de responsabilidad civil se debe a que los criterios establecidos en el artículo 27 de la LEPDP, a tener en cuenta para las sanciones

¹²⁴Aunque autores como Tamayo Jaramillo(2007:33-35) afirma que la carga probatoria de la imputación de responsa

¹²⁵En efecto en la sentencia T-279 de 2002 se afirmó que "(...) debidamente administrada se realice bajo dos principios, llamados a operar bajo la premisa de la posición de garante de la entidad administradora y del peticionario: el principio de responsabilidad compartida, según el cual, tanto quien solicita la información como quien la suministra, desarrollen su conducta teniendo en cuenta la existencia de un interés protegido en cabeza del titular del dato. Y el principio de cargas mutuas, según el cual, a mayor información solicitada por un tercero, mayor detalle sobre su identidad y sobre la finalidad de la información."

¹²⁶Explica Mantilla (2007) que "(...) una obligación de resultado conlleva un régimen objetivo de responsabilidad puesto que el acreedor insatisfecho no está obligado a probar la culpa del deudor incumplido y este tampoco puede exonerarse demostrando ausencia de culpa", esto excluye la prueba de causa extraña. Para diferenciar esta clase de obligación de las de medio hay tres maneras: i) declaración expresa del legislador, ii) acuerdo de las partes y iii) por "(...) la mayor o menor probabilidad que tenga el deudor de alcanzar el objetivo último buscado por el acreedor al celebrar el contrato"(Tamayo,2007:539)

por parte de la Superintendencia de Industria y Comercio, son mayormente objetivos y no tomaron en cuenta factores subjetivos como la culpa o el dolo. Sin embargo en el análisis de la responsabilidad civil se tendrá en cuenta la configuración del ordenamiento jurídico colombiano respecto a la primacía del principio de la culpa para imputar la misma para imputar el tipo de responsabilidad más adecuado al caso debido a la falta de regulación expresa.

La responsabilidad civil proyecta sobre el derecho de la protección de datos personales la misma estructura teórica: sujetos, conducta, nexo causal y en algunas ocasiones, daño. A continuación se pasa a describir la aplicación de la responsabilidad civil en dos partes: requisitos de la responsabilidad civil y alcance de la responsabilidad civil.

ii) Requisitos de la responsabilidad civil

Para que surja la responsabilidad civil se requiere del daño, el nexo causal y la conducta.

El daño: El sufrimiento, afectación o destrucción del interés jurídico se denomina daño, definido como “la alteración negativa de un estado de cosas existentes” (Henao ,1998:84), cuyas consecuencias implicaría una serie de acontecimientos desfavorables para la persona desde el plano económico o moral, definido como un perjuicio, entendido como “(...) el conjunto de elementos que aparecen como las diversas consecuencias que se derivan del daño para la víctima del mismo” (Bénoit, “Essai sur les conditions de la responsabilité en droit public et privé”, citado por Henao,1998:77)

El objeto del daño es la afectación del interés humano tutelado jurídicamente, entendido como lo manifiesta De Cupis (1978:111) de “necesidad, experimentada por uno o varios sujetos determinados, que venga satisfecha mediante un bien”. Se habla de interés humano en general, pero se tomará en cuenta aquel interés de un sujeto o sujetos específicos e individuales y con potencial valor patrimonial o carente de él, pero cuyo rasgo común es ser de interés para el ordenamiento jurídico. El daño se presenta como un puente entre el hecho

generador de este y la norma jurídica y es importante para determinar la intensidad de la afectación de la norma jurídica (De Cupis, 1978:83 y ss.)

De Cupis (1978:153) explica las diferencias entre daño contractual frente al extracontractual:

“Ciertamente que el vínculo obligatorio contractual mediante la integración que hemos visto, puede extenderse más allá de cuanto han previsto las partes del contrato, pero no puede llegar a comprender lo que es totalmente extraño a la índole de la prestación convenida”

En la protección de datos personales la persona es lesionada primeramente en su aspecto moral, afectando el derecho a la intimidad y luego las consecuencias que tenga el uso de los datos personales, que pueden ser también morales, como la afectación del buen nombre y de la estima que se tiene a sí misma. También puede incurrirse en lesiones económicas con el uso de esa información para fines distintos porque perdió fuentes de ingresos o lucro o generó gastos imprevistos.

Los sujetos: En cuanto a este aspecto quien sea civilmente responsable será el que haya cometido la afectación con su conducta , esta no se encuentre permitida por el ordenamiento jurídico y además pueda concluirse que lo produjo mediante la figura del nexo de causalidad.

En cuanto a los sujetos se afirma que el responsable del tratamiento responderá indirectamente de los daños que haya causado el encargado del tratamiento, siempre que corresponde al mismo origen, esto es una conducta realizada en cumplimiento del contrato de tratamiento de datos personales acordado entre ambos, en este caso habrá solidaridad de las obligaciones. Esto se justifica a partir de considerar al tratamiento de datos personales como actividad mercantil, por lo tanto es aplicable el artículo 825 del C. de Co. que hace solidarios a quienes se han comprometido a la misma prestación.

Ahora respecto a daños producidos por diferente causa Tamayo Jaramillo (2007:61) opina lo siguiente: “Tratándose de daños diferentes, es claro que cada responsable responde por lo que dañó”. Esto significa que si se produce el daño con fuente diferente al contrato que rige la relación entre el responsable del tratamiento y el titular del dato, algo por ejemplo que el titular facilite datos directos al encargado, sin que lo sepa el responsable, quien responderá por el uso indebido será el primero.

¿Qué ocurre cuando el daño es causado por una persona a cargo del responsable o tratamiento de datos personales? Al respecto es aplicable la figura de responsable por el hecho ajeno que Tamayo Jaramillo (2007:656 y siguientes) define que ocurre cuando se ocasiona un daño “(...) imputable causalmente a su propio comportamiento, sino también cuando dicho daño ha sido causado por una tercera persona (...)” con la cual tiene una relación contractual para ejecutar las obligaciones pactadas.

La Conducta: Al respecto nos amparamos en la idea afirmada por el profesor Javier Tamayo (2007:188) respecto a que es esencial para definir la responsabilidad el tipo de conducta que ejecutó (acción u omisión) debido a que los hechos ilícitos de la responsabilidad objetiva quedarían excluidos cuando se usen culpa y la noción sola de hecho ilícito deja incomprendida a quien se le imputa la responsabilidad pues no fue cometido sólo. “El hecho ilícito siempre está precedido, desde el punto de vista psicológico o filosófico, de un acto humano (...) que no pretende crear efectos jurídicos, pero que de hecho los crea porque se produce un daño en forma ilícita”. El comportamiento, con efectos jurídicos ilícitos, de las personas es lo que genera responsabilidad civil.

La conducta puede ser con dolo, entendido como *la intención positiva de inferir injuria a la persona* o culpa, que es el desprecio de una persona del riesgo latente que van correr los bienes jurídicos de los demás con su actuación imprudente¹²⁷ o negligente¹²⁸ o sin pericia¹²⁹ o

¹²⁷Sobre esta dice Javier Tamayo(2007:227): “Podríamos definir la imprudencia como la temeridad o ligereza con que el sujeto realiza una conducta, bien sea porque no prevea los efectos de la misma, debiéndolos prever, o porque a pesar de haberlos previstos se confía en poderlos evitar”

¹²⁸Sobre está dice Javier Tamayo(2007:227): “La negligencia, en cambio, es el descuido con que el agente realiza sus actividades”

en el incumplimiento de obligaciones emanados de una norma (Tamayo, 2007:221-224). La culpa“(…) es un elemento meramente subjetivo que conlleva al agente a comportarse como no lo haría un hombre prudente y avisado” (Tamayo, 2007:193), calificada mediante el grado de culpa, que en el código civil (Art.63) está en leve, grave y levísima. Estos grados de culpa inciden en el monto de la indemnización pues permite determinar cuánto contribuyó a la producción del daño el demandante. Pese a que se defiende el régimen de responsabilidad objetivo para el indebido tratamiento de datos personales, creemos convenientes las anteriores pinceladas, dado que legalmente la responsabilidad civil es subjetiva mayoritariamente en Colombia.

Ahora en cuanto a quien comete el daño, tomaremos el criterio según el grado de control que puede tener la persona en la materialización del daño; la teoría de la responsabilidad civil distingue en directa e indirecta. La primera cuando se responde por el hecho propio y la segunda cuando el daño causado por el hecho de una tercera persona o bien del daño originado en el hecho de las cosas (aquel daño cuya génesis se encuentra en la omisión inicial de un acto humano) o bien como dice De Cupis (1978:130)“(…) participación del ser humano en el desenvolvimiento del proceso dañoso derivado de las cosas”.

La responsabilidad directa puede ser contractual o extracontractual, mientras que la indirecta casi siempre será extracontractual.

La conducta en el tratamiento indebido de datos personales es variada, tentativamente podrían agruparse las conductas en tres: i) una intrusión sin permiso en la base de datos, ii) la alteración o entrega de la base de datos por parte de los dependientes del responsable o encargado, iii) el engaño o fraude para obtención de los datos y tratamiento de datos personales.

En el primer caso, sobre la intrusión sin permiso en la base de datos se presenta en los casos de intentos de violación a la seguridad de la información con fines ilícitos o de obtención de provecho con el acceso al dato personal. La responsabilidad será objetiva

¹²⁹Javier Tamayo(2007:227):“(…) consiste en la ausencia de conocimientos con que el agente realiza la conducta que no debió haber realizado”

contractual entre el responsable del tratamiento y el titular y objetiva extracontractual entre este y el encargado del tratamiento, frente al causante del daño habría una responsabilidad extracontractual con culpa por haber generado la situación dañosa.

El segundo caso ocurre cuando el dependiente o el mismo responsable realiza acciones que no están explícitas en las políticas, como agregar datos falsos o modificarlos o hacerlos público.

En el tercer caso, el encargado o responsable mediante la confianza que ya se tiene depositada u otros medios hace que de autorizaciones para usos que la persona posiblemente no consentiría o que se le digan unas finalidades del uso del dato y se usen para otro. Cabe aclarar que si existe la autorización consciente de los datos personales podría afirmarse que no se imputaría responsabilidad, sin embargo deben mirarse los otros principios de administración de datos personales para comprender hasta que punto su incumplimiento genera daños para el titular

Nexo causal: Es la vinculación jurídica que existe entre la conducta de una persona y las consecuencias que generó sobre un bien jurídico.

En el aspecto contractual según Tamayo Jaramillo (2007:78) hay que distinguir entre daños vinculado por incumplimiento oportuno o completo del contrato y los daños producidos con ocasión de la ejecución del contrato. Los primeros se generan cuando no se cumple adecuadamente las cláusulas fijadas en la política de tratamiento de datos personales, están relacionadas con la finalidad y los segundos se generan con independencia del cumplimiento del contrato pero si porque el tratamiento de datos personales ocasionó afectaciones a la persona que no estaban previstas o son inconstitucionales.

Para el caso del tratamiento indebido de datos personales el nexo de causalidad se deduce a partir de la conducta desplegada por las personas que rodean al titular del dato personal afectado. Por ejemplo, cuando la persona acude a un sitio web para comprar un par de libros, facilita sus datos comerciales y su tarjeta de crédito en cumplimiento del contrato de

venta al momento de pagar, tiempo después se entera acerca de unos gastos excesivos durante ese mismo día, le pide al banco información, identifica que se realizaron desde un computador cuya IP está vinculada al domicilio de la empresa de comercio electrónico, esta responderá contractualmente porque si bien cumplió su obligación principal de entregar la cosa, al ser un contrato de venta, al no cumplir con las previsiones de seguridad (que estaban incluidas dentro de su política de tratamiento de la información personal), obligación accesoria pero necesaria con ocasión de la ejecución del contrato, causó un perjuicio enorme en el patrimonio del titular del dato. Esta tesis es sostenible en tanto que la situación ocurre entre dos sucesos de la relación jurídica: el que asegura el vínculo jurídico mediante el pago de la cosa y su perfeccionamiento con la entrega de la mercancía.

c) Acción penal

i) La Ciber-criminalidad: Una introducción

Como bien se mencionó en la sección sobre el origen del derecho al Habeas Data fue el uso indiscriminado y abusivo de los datos personales sumado a la revolución tecnológica que masificó su utilización en todos los ámbitos, también impactó en otros ámbitos del derecho. En efecto la única reacción no provino solamente del derecho constitucional, también el derecho penal aportó su grano de arena al observar que ciertas conductas tenían un daño enorme a la paz y la armonía social. En conjunto el Estado formuló una respuesta para garantizar la seguridad en internet y en los sistemas informáticas de todas las empresas e instituciones para asegurar la protección de las personas.¹³⁰

Esas conductas eran cometidas con dolo o culpa y representaban riesgos importantes para la confianza de las personas en el uso de los sistemas informático (Posada, 2006:14), lo que en últimas afectaba este sector como potencial generador de beneficios sociales y económicos a la población. Los gobiernos se han preocupado por reprimir estas conductas, creando tipos penales específicos que castigan fuertemente el uso de los medios informáticos

¹³⁰Esto en desarrollo del fin esencial del Estado establecido en el artículo 2 de la Constitución, el artículo 66 de la ley 906 de 2004 que desarrolla la titularidad del Estado para conservar los bienes de las personas a través de la acción penal, que recaee en la Fiscalía General de la Nación.

para la comisión de ilícitos. Esto último es lo que se conoce como *cibercriminalidad* o *criminalidad informática*, conductas que si bien se afirma que se deben cometerse bajo el principio de culpabilidad lo que está ocurriendo es que se describen normativamente como tipos de peligro en abstracto, lo cual contradiría ostensiblemente la primera afirmación.

El problema de la cibercriminalidad ha sido definido por el profesor Posada Maya (2006:16 y 22) en los siguientes términos:

“Por supuesto, la criminalización primaria de las conductas peligrosas dirigidas a afectar los intereses informáticos, los intereses de los usuarios y propietarios de los sistemas informáticos, los intereses generales, de terceros y del Estado a través de dichos medios y sus instrumentos, resulta un problema sustancialmente político-criminal que —como cualquiera otra decisión en este sentido— implica valorar la utilidad real (por oposición a la simbólica) y la correcta legitimidad de la penalización de dichas conductas, desde las diversas perspectivas sociales, económicas y políticas que intervienen en la realidad colombiana, con el propósito de lograr una legislación dinámica en la materia.

(...)

Por tal motivo, la categoría de ‘delitos informáticos o Cibercrímenes’ está llamada por el momento —en nuestro medio— a hacer parte de otras clasificaciones materiales de corte criminológico en el ámbito penal —p. Ej.: los delitos de “cuello blanco o white collar crimes y/o High-tech crimes”—, que abarcan un sinnúmero de comportamientos lesivos contra bienes jurídicos variados, sobre todo en el ámbito de los intereses patrimoniales y socio-económicos.

(...)

Con tal punto de partida, los delitos informáticos constituirán figuras delictivas autónomas (*delicta sui generis*), de peligro y en blanco, aplicables de forma preferente cuando se vulneren las funciones informáticas referidas a la información (entendida

como bien inmaterial público y nuevo paradigma económico), frente a otras conductas que vulneren bienes jurídicos personales o personalísimos de forma incidental²⁹. Dicho lo cual, el problema jurídico se traslada, no solo a la cuestión de la legitimidad de las modalidades típicas necesarias para proteger dicho interés social como bien jurídico, sino también al tratamiento que se debe dar, conforme a las reglas que rigen la unidad o pluralidad de tipicidades, a las conductas que trascienden la afectación de la información y vulneren —al tiempo— otros bienes jurídicos como la intimidad personal”

El debate acerca de la expansión del derecho penal a nuevos ámbitos con la creación de tipos penales autónomos no es un aspecto a tratar en este trabajo¹³¹. Sin embargo no estamos de acuerdo en que puede aumentarse la seguridad informática a través de la penalización de conductas cometidas e inclusive de la asignación de la actividad informática como una actividad de peligro, lo que denota una fuerte carga social negativa¹³². Simplemente las tecnologías no son buenas o malas, son ciertamente las personas quienes tienen intereses ilícitos al cometer las conductas: obtener información confidencial, obstruir el desempeño y gestión de actividades empresariales o gubernamentales, cometer hurto de dinero o propiedades a través de la modificación de los sistemas de información. Esto deja la cuestión principalmente a una autorregulación del sector privado, quien ya ha definido estándares de seguridad de información claramente reconocidos por las empresas de internet como válidos.

¹³¹Al respecto de la problemática resume Posada Maya (2006:18) que la dogmática penal debe ponerse de acuerdo en dos temáticas: “(...) en primer lugar, la comunidad jurídica nacional debe alcanzar determinados consensos policriminales en la materia, que procuren una racionalización progresiva de las medidas preventivas y punitivas que deba adoptar la legislación en el contexto económico colombiano, desde luego, atendidas las recomendaciones internacionales en la materia. Y, en segundo lugar, es necesario que nuestro medio tome conciencia de la importancia de lograr altos niveles de autorregulación privada en gestión de seguridad informática, pues sólo de este modo se podrán identificar y legitimar los espacios de intervención punitiva necesitados de protección penal, de conformidad con las exigencias de subsidiariedad y fragmentariedad, una vez agotadas otras instancias legales de prevención (paradigma de contención).”

¹³²Aunque otros autores explican la necesidad de un “derecho penal corporativo” para sancionar las conductas cometidas por individuos a favor de las empresas porque las “(...) personas jurídicas en la realidad tienen voluntad, poseen intereses propios distintos a los de las personas físicas, desarrollan una actividad propia y por ello pueden cometer delitos, son responsables por el actuar de sus órganos y deben soportar las consecuencias penales.” Ver más en: Castro Ospina, S. *Algunos aspectos dogmáticos de la delincuencia informática*. Disponible en: <http://www.delitosinformaticos.com/02/2008/noticias/algunos-aspectos-dogmaticos-de-la-delincuencia-informatica>

La misma Corte Constitucional aprueba la existencia de este derecho penal, mediante sentencia C-320 de 1998 afirmó que “(...) La sanción penal limitada a los gestores, tan solo representa una parcial sanción punitiva, si el beneficiario real del ilícito cuando coincide con la persona jurídica se rodea de una suerte de inmunidad. La mera indemnización de perjuicios, como compensación patrimonial, o la sanción de orden administrativo, no expresan de manera suficiente la estigmatización de las conductas antisociales que se tipifican como delitos”.

El único aspecto central es que los dos bienes jurídicos tutelados son la: seguridad de la información y la seguridad de los sistemas informáticos. Esto permite comprender que hay dos tipos penales informáticos: tipos penales con conductas – entiéndase verbo rector - tradicionales cometidas mediante técnicas informáticas para afectar o destruir software y delitos informáticos en sentido propio, como aquellos que afectan “(...) integridad y la disponibilidad de datos o información” (Posada, 2006:19).¹³³ Aunque el profesor Posada Maya afirma que podría presentarse un concurso de conductas punibles, donde los delitos informáticos pasan a ser meros instrumentos para lograr un fin criminal mayor¹³⁴, porque a través de una conducta se afectan múltiples bienes jurídicos contemplados en varios tipos penales, por ello “(...) se puede hablar de unidades de conducta de naturaleza pluriofensiva (pues afectan diversos bienes jurídicos tutelados), que probablemente configurarán una pluralidad de tipicidades entre ‘computer crimes’, ‘computer-related-crimes’ y conductas punibles tradicionales.”

Adicionalmente debe destacarse que los encargados y responsables del tratamiento de la información personal por virtud del principio de seguridad y acceso restringido cumplen los supuestos de hecho del artículo 25 del Código Penal colombiano sobre la posición de garante para “evitar que puedan realizarse conductas lesivas por parte de terceros. En consecuencia, pese a que la víctima con posterioridad a la creación de un riesgo por un tercero actúe en forma imprudente, ello no exonerará de responsabilidad a quien tenía el deber de salvaguardar la incolumidad del objeto custodiado frente a cualquier riesgo.” (Castro, 2006) Esto aplica para los tipos penales de los artículos 269G, 269F, 269C, 269B y 269A.

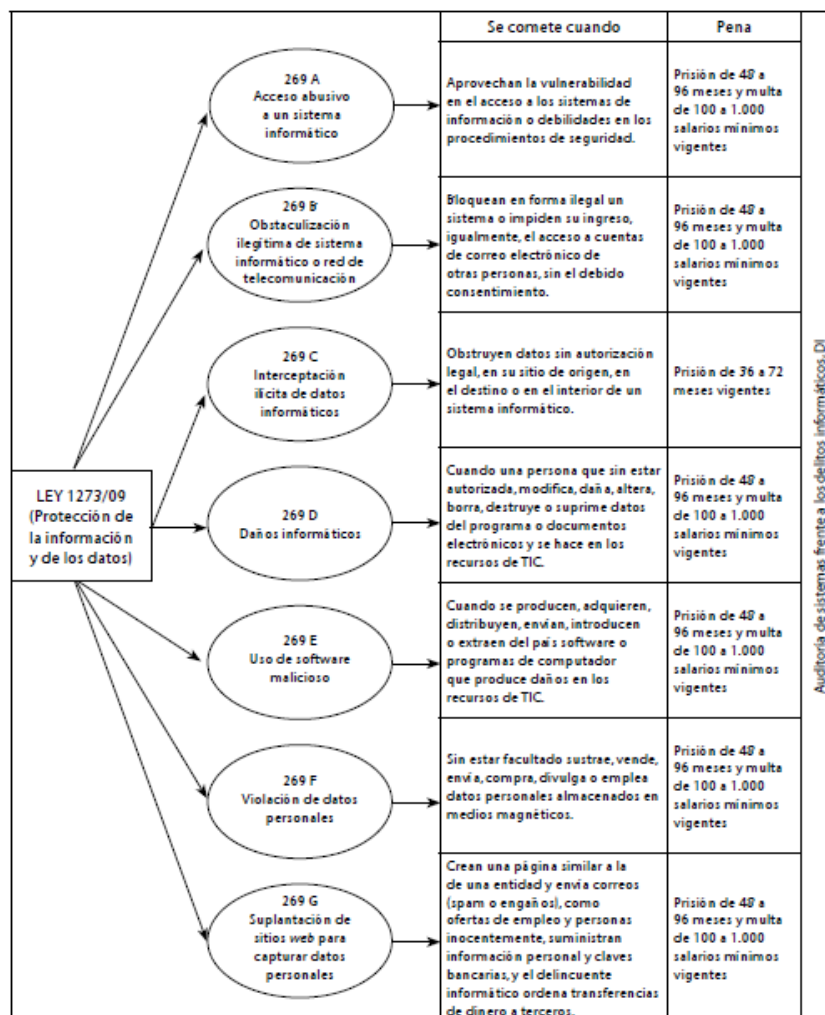
¹³³Clasificación que es corroborada por Julio Telléz quien afirma que los delitos informáticos son de medio y o instrumento y de fin u objetivo. Donde las primeras se incluyen aquellos que tienen como medio para la comisión de delitos a la informática y los segundos aquellos que buscan atacar directamente a manifestaciones de esta como las aplicaciones web, móviles, sistemas informáticos, dispositivos móviles, dispositivos de escritorio. Ver más en: Chiaravalloti, Alicia; Levene, Ricardo. Introducción a los delitos informáticos, tipos y legislación Madrid: Portaley nuevas tecnologías. Disponible en: <http://delitosinformaticos.com/delitos/delitosinformaticos.shtml>

¹³⁴Por ejemplo atacar un sistema informático para borrar los antecedentes penales de una persona o facilitar el ingreso a una caja fuerte bancaria asegurada remotamente.

De manera breve se planteó el significado actual en la dogmática penal de la cibercriminalidad, ahora se pasa a describir los tipos penales informáticos que afectan el bien jurídico denominado “de la protección de la información y los datos” que creó la ley 1273 de 2009 relacionados directamente con el indebido tratamiento de datos personales.

ii) La legislación penal informática en Colombia

A continuación se expone de manera sintética los tipos penales para un a vista rápida al respecto según lo expone Ojeada (2010: 55):



*iii) Acceso abusivo a un sistema informático*¹³⁵

Para la comisión de esta conducta se requiere el ingreso sin permiso al sistema informático, bien puede realizarse sin las credenciales facilitadas para el acceso a través de un “ingreso forzado” quebrando los protocolos de seguridad fijados del sistema o a través de la consecución ilegítima de credenciales de acceso. El ingreso al sistema sin autorización o contra la voluntad del administrador del sistema informático y su permanencia “dentro” denota una intención dolosa de hacer daño; claramente se tiene “(...) la posibilidad fáctica – *al menos un instante* – de obtener servicios o disponer de la información existente y retirarla del mismo; con lo cual, se crea un peligro verificable y concreto para el titular de los bienes jurídicos” (Posada, 2006:24). Al respecto Posada Maya (2006:24) afirma que es pieza clave el permiso de este último porque “es lo que permite la conexión normal al medio informático y lucrarse de manera lícita (aun cuando sea el mismo prestador del servicio sin legitimidad, arguyendo razones de verificación).”

Pueden excluirse los “ingresos inocentes”, aquellos que ocurren de manera incidental o bajo error del mismo sistema y el usuario permanece allí sin percatarse de que es una zona no autorizada o sin intención de provocar una alteración en el sistema. Así también se excluyen los casos de *hacking* ético, que son intrusiones permitidas a personas o empresas externas con miras a detectar problemas de seguridad que luego reportan a los administradores del software. Aunque por el *mero peligro* que viene rodeando al tipo penal probablemente será típica su conducta y antijurídica en ambos casos, no cumplirá con el elemento de responsabilidad penal de la culpabilidad.

Bajo este tipo penal se protegen los derechos al debido tratamiento de datos personales, en especial los principios de legalidad, seguridad y acceso restringido de la información. Estos principios cuando son vulnerados por terceros hacen peligrar el almacenamiento y tratamiento de datos personales puesto que, como se mencionó antes, se abre la posibilidad de conocer información a la cual no ha sido autorizado el acceso o lo hace por fuera de lo acordado, esto

¹³⁵Artículo 269A: *Acceso abusivo a un sistema informático*. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

último para el caso de abuso del deber de confianza cuando es un subordinado del encargado del tratamiento de datos personales.

Es un tipo penal de conducta instantánea pues se sanciona el hecho de introducirse simplemente en el sistema de información de manera abusiva, sin contemplar que sea para un resultado específico.

*iv) Violación de datos personales*¹³⁶

Este delito se establece para la protección del honor, la honra y la intimidad que se ven potencialmente en riesgo con el acceso desautorizado a los datos personales del titular, sin que medie una relación contractual o legal que justifique.

Tiene una amplitud el concepto de violación pues incluye desde conductas intrusivas hasta aquellas que no están permitidas dentro de la política de tratamiento de la información personal.

Este tipo penal es el que directamente protege al titular del dato personal de tratamientos indebidos pues se centra en las conductas realizadas sin autorización del titular, describiendo con detalle, dejando de lado los medios o maneras en que puede obtener la información.

Ahora los principios administradores que se encuentran a buen resguardo son el de libertad, el de legalidad, el de finalidad, confidencialidad, circulación y acceso restringido.

¹³⁶ Artículo 269F: *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

v) *Daño informático*¹³⁷

Dentro de este tipo penal está inmersa intromisiones lesivas con efecto de modificación de la base de datos, del sistema informático o de los protocolos de seguridad establecidos, intentando con ello lograr un propósito provechoso o simplemente para probar la calidad de los conocimientos técnicos en intrusión de sistemas o la seguridad de este último. El profesor Ricardo Posada Maya lo enmarca dentro de las intrusiones informáticas con efectos modificatorios, “(...)más allá de la simple motivación de superar – por superar – las medias de seguridad electrónicas dispuestas”.

Ahora analizando el enunciado normativo, el supuesto de hecho incluye la intrusión con miras a modificar los datos informáticos, circunstancia que una vez realizada y usada la nueva información implantada genera errores en la identidad de la persona. Para efectos penales el ilícito ya fue cometido desde que la modificó (destruya, dañe, borre, deteriore, altere o suprima), pero para efectos del Habeas Data, este es vulnerado cuando el sistema utiliza la información con consecuencias desastrosas para la persona de quien ahora el banco de datos tiene información que viola el principio de calidad de la información.

Es un tipo penal de resultado, sino logra realizarse la afectación o perjuicio en algunas de las conductas descritas (destruir, borrar, dañar, deteriorar, alterar, suprimir) la conducta se transformaría en acceso abusivo a sistema informático que tipifica el artículo 269A. En caso de que se consiga podría hablarse de un concurso de conductas con el artículo 269B por hacer que funcione mal el sistema informático.

Frente a este tipo penal los principios del habeas data afectados son el de legalidad en el tratamiento, seguridad, calidad y veracidad

¹³⁷Artículo 269D: *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

vi) *Obstaculización ilegítima de sistema informático o red de telecomunicación*¹³⁸

Este tipo penal es bastante semejante al de daño informático con la diferencia de que su fin es impedir el buen funcionamiento del sistema informático o de los datos que en él están contenidos. En el ejercicio de este impedimento puede provocar daños permanentes que hagan inservible el sistema, es decir que lo destruyan, frente a lo cual podría haber un concurso aparente de conductas punibles, pues quedaría subsumido por el daño informático, dado que este tipo penal contempla un resultado específico más amplio, que es evidente con su nombre. Adicionalmente podría impedir que funcione por uno momento el sistema informático.

Aunque está más cerca del tipo penal de *sabotaje* regulado en el artículo 199 del Código penal colombiano porque “(...) puede resultar en el daño del contenido de los sistemas informáticos y asimilados (...) por vía electrónica utilizando programas dañinos u otros recursos” (Posada, 2006:41) pues ambos tienen el fin de detener el normal funcionamiento del sistema informático y del trabajo.

vii) *Interceptación de datos informáticos*¹³⁹

Este es un tipo penal especializado que protege la transferencia de información entre el responsable y el encargado, cuando se realiza legítimamente, de las intrusiones informáticas con miras a conocer lo que se transmite o hacer que se desvíe la “ruta de guardado” de la información o comunicación. Igualmente cuando ocurre la interceptación entre el dispositivo tecnológico de la persona titular del dato personal y el servidor del encargado del tratamiento, a quien le entrega los datos por medio de software especializados o las famosas apps.

¹³⁸Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación*. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

¹³⁹Artículo 269C: *Interceptación de datos informáticos*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

El sujeto es indeterminado y no calificado¹⁴⁰, los ingredientes normativos están los datos informáticos (junto a las ondas electromagnéticas que no son pertinentes) y el hecho de que se realice la conducta sin autorización judicial.

En este tipo penal se está afectando el principio de confidencialidad, seguridad y acceso restringido a la información. Habrá que mirar si este último vulnerado fue por negligencia del administrador de bases de datos en los protocolos de seguridad de la información, lo cual generaría una responsabilidad civil contractual por incumplimiento a sus políticas de tratamiento de la información.

En este tipo penal faltó incluir ingredientes normativos respecto al tipo de información que se haya interceptado, puesto que para la LEPDP están fijados distintos grados de intensidad en el cumplimiento de los principios a partir del tipo de dato personal tratado, lo que se excluye del enunciado normativo. “En efecto, no es lo mismo revelar o divulgar información sobre un sujeto mayor de edad que información relativa a un menor de edad o un incapaz que se encuentre en situación de indefensión frente a dichas actividades.” (Posada, 2006:35)

No existen ingredientes normativos salvo la calificación del sujeto, de la finalidad y del objeto material sobre el que recae la conducta.

¹⁴⁰Es así para incluir al sujeto común y al sujeto responsable, pues este puede ser contratado por el primero para obtener la información, lo cual haría al primero en determinador del segundo. De esta manera se acoge la sugerencias al respecto realizadas por el profesor Ricardo Posada en su artículo “Aproximación a la criminalidad informática en Colombia”(ver bibliografía)

viii) *Suplantación de sitios web para capturar datos personales*¹⁴¹

Este delito informático pertenece a la modalidad de engaño o manipulación usando medios informáticos o páginas de internet o programas que se hacen instalar en los dispositivos móviles. El profesor Ricardo Posada Maya (2006:42) da algunos interesantes ejemplos aplicados a la captura de datos para cometer delitos patrimoniales mayormente como al *financial institution fraud*, *el gamming fraud*, *el advance fee fraud*, entre otros.

Si bien este tipo penal es de resultado cabe aclarar que puede convertirse en uno de conducta permanente, pues al respecto dice Rodríguez Gómez (cit. por Posada,2006:44) que si se hace a cuenta gotas poco a poco, al final nos encontramos con una gran cantidad de información que ha sido recopilada indebidamente sin que nos percatemos acerca de ello.

La diferencia es que en esta suplantación no se busca obtener un provecho económico directo sino los datos personales de individuos, para usarlos con fines diferentes. En este tipo penal se están vulnerando los principios de finalidad, de legalidad, de confidencialidad y de transparencia.

El ingrediente normativo es el “objeto ilícito” dentro del cual caben dos tipos de crimen informático: el fraude informático, en el primer inciso y la falsedad informática, en el segundo inciso. El fraude informático consiste en obtener mediante engaños de un tercero la información o los datos personales que no entregaría si se le hace público los fines. La falsedad informática si bien implica el engaño, este ocurre con relación a aspectos en los cuales confía por naturaleza la persona para entregar sus datos: correos de su entidad bancaria, de su empleador, de un amigo o conocido, según Posada(2006:46) implica “(...) el uso

¹⁴¹Artículo 269G: *Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

malicioso de los resultados de un proceso de elaboración o transmisión de datos almacenados, mediante la configuración de los programas o del software, conductas que generen información falsa a fin de practicar engaños en el tráfico jurídico mediante documentos”¹⁴²

Con la comisión de la conducta de este tipo penal se están vulnerando los principios de administración de transparencia, veracidad, libertad y confidencialidad.

Tutela administrativa

El estado en desarrollo de sus fines constitucionales, entre los que se encuentra la protección de los derechos fundamentales y la promoción del interés general, ejerce una función de supervisión y ordenación de la sociedad. Lo realiza a través de múltiples órganos con competencias asignadas por la Constitución o por la ley.

En materia de protección de datos personales las autoridades públicas que tienen dicha competencia son: el Defensor del Pueblo, la Superintendencia de Industria y Comercio como Autoridad de Protección de Datos en materia general, que cede a la Superintendencia Financiera en materia de datos comerciales, crediticios y financieros en cuanto a entes vigilados por esta última y la Procuraduría General de la Nación junto a las oficinas de control interno disciplinario de cada entidad pública y las personerías en las investigaciones y sanciones contra servidores públicos.

En cuanto a la tutela administrativa es pertinente aclarar que las anteriores autoridades públicas tienen un papel específico dentro del engranaje de protección de datos personales. Así pueden cumplir una o varias de las siguientes funciones: función orientadora del Régimen general de Protección de datos personales, Función de promoción de la protección de este del derecho fundamental de habeas data, función sancionatoria ante el incumplimiento del

¹⁴²Desde el punto de vista jurídico un sitio web en sus distintas variantes, que describe el tipo penal, es un mensaje de datos, lo cual es tratado en el Código General del Proceso como medio de prueba documental.

régimen legal por los responsables y encargados de naturaleza privada o pública. A continuación se explicará con el siguiente cuadro:

Funciones de las Autoridades Públicas para la protección de datos personales

Autoridad Pública	Función Régimen de Habeas Data	Descripción de la función
Procuraduría General de la Nación	Función sancionatoria por incumplimiento de la ley	En ejercicio de la potestad disciplinaria preferente (artículo 3 ley 734 de 2002) preferente pueden investigar y sancionar a los servidores públicos de entidades públicas que tratan datos personales o a particulares en ejercicio de funciones públicas (artículo 53 ley 734 de 2002)
Defensor del Pueblo	Función de promoción de la protección de derecho de habeas data.	Se encarga de promover tutelas por violación a este derecho y de difundir el conocimiento de este derecho
Superintendencia de Industria y Comercio	Función Orientadora del régimen legal de protección de datos personales	Se encarga de dar las orientaciones sobre la aplicación de la ley, investigar las violaciones de la LEPDP, sancionar a los encargados y fuente del tratamiento de naturaleza privada. Ley 1581 de 2012. También es competente en los datos comerciales, financieros y crediticios que provienen de terceros países y que no ingresen a una filial que esté bajo vigilancia de la Superfinanciera.
Superintendencia Financiera	Función Orientadora del régimen legal de protección de datos personales	Se encarga de dar las orientaciones sobre la aplicación de la ley, investigar las violaciones de la LEPDP, sancionar a los operadores, usuarios y fuentes de la información de naturaleza privada que están bajo vigilancia de esta que traten datos comerciales, financieros y crediticios (Inciso 2° Artículo 17 ley 1266 de 2008)
Oficinas de Control Interno Disciplinario en las entidades	Función sancionatoria por incumplimiento de la ley	En ejercicio de la potestad disciplinaria (artículo 2° y 76 de la ley 734 de 2002) pueden investigar y sancionar asuntos disciplinarios de los servidores públicos vinculados a la entidad.

públicas		
Consejo Superior de la Judicatura	Función sancionatoria por incumplimiento de la ley a los abogados	Investiga y sanciona a los funcionarios de la rama judicial (artículo 193 de la ley 734 de 2002) que cometan faltas disciplinarias referentes al indebido tratamiento de datos personales.
Personerías municipales y distritales	Función sancionatoria por incumplimiento de la ley	Ejercen poder sancionatorio frente a los servidores públicos municipales.(Inciso 4° del artículo 3 de la ley 734 de 2002)

Fuente: Camilo José Puello Rincón. Junio de 2016

a) Defensor del Pueblo

El defensor del pueblo como funcionario encargado de proteger y salvaguardar los derechos fundamentales puede hacerlo de muchas maneras. Promoviendo el conocimiento de los derechos fundamentales y asistiendo a las personas en la defensa de ellos (282-1 constitucional), si lo solicitan, puede interponer en su nombre de la acción de tutela (282-3 constitucional).

En los artículo 46 a 50 del decreto 2591 de 1991 se regula la modalidad de intervención y la posibilidad de que lo hagan los personeros municipales en su nombre por delegación, así como la asistencia jurídica a las personas. El Defensor del Pueblo está legitimado para iniciar a nombre de cualquier persona residente en Colombia¹⁴³ o de nacionales residenciados en el exterior¹⁴⁴, intervenir como parte¹⁴⁵ en un proceso constitucional de protección de derechos fundamentales de manera directa o por delegación en los personeros municipales¹⁴⁶

¹⁴³ Artículo 51. Colombianos residentes en el exterior. El colombiano que resida en el exterior, cuyos derechos fundamentales estén siendo amenazados o violados por una autoridad pública de la República de Colombia, podrá interponer acción de tutela por intermedio del Defensor del Pueblo, de conformidad con lo establecido en el presente Decreto.DECRETO 2591 DE 1991.

¹⁴⁴ Artículo 46. Legitimación. El Defensor del Pueblo podrá sin perjuicio del derecho que asiste a los interesados, interponer la acción de tutela en nombre de cualquier persona que se lo solicite o que esté en situación de desamparo e indefensión. DECRETO 2591 DE 1991.

¹⁴⁵ Artículo 47. Parte. Cuando el Defensor del Pueblo interponga la acción de tutela será, junto con el agraviado, parte en el proceso.DECRETO 2591 DE 1991.

¹⁴⁶ Artículo 49. Delegación en personeros. En cada municipio, el personero en su calidad de defensor en la respectiva entidad territorial podrá por delegación expresa del Defensor del Pueblo, interponer acciones de tutela o representarlo en las que éste interponga directamente.DECRETO 2591 DE 1991.

b) Superintendencia de Industria y Comercio: Autoridad Nacional de Protección de datos personales

i) Poder de policía administrativa y poder sancionador del Estado

La Superintendencias en ejercicio de la potestad delegada por el Presidente de la República cumplen funciones de inspección, vigilancia y control de varios sectores de la sociedad. La encargada de vigilar el aspecto de habeas data es la Superintendencia de Industria y Comercio y la Superintendencia Financiera para entidades vigiladas por ella que traten datos personales inherentes a su labor (inciso 2° Art.17) y la Unidad Administrativa Especial de Aeronáutica Civil¹⁴⁷. Está excluida la competencia sancionatoria sobre entidades públicas, que le corresponde a la Procuraduría General de la Nación, personeros municipales y a las oficinas de control interno de las entidades; el Consejo Superior de la Judicatura para servidores públicos judiciales. En adelante se nombrarán indistintamente como Autoridad Pública de Protección de datos personales y se diferenciará cuando se haga referencia a una facultad específica o diferente relacionada con su labor de protección de datos personales, el motivo es que la LEPDP, la ley 1266 de 2008 y las otras leyes asignan un procedimiento común para todas sus actuaciones: el que establece la ley 1437 de 2011.

La Corte denomina genéricamente este poder de inspección, vigilancia y control como poder de policía y poder sancionador, lo definió así en la sentencia C-748 de 2011:

“El poder sancionador estatal ha sido definido como un instrumento de autoprotección, en cuanto contribuye a preservar el orden jurídico institucional mediante la asignación de competencias a la administración que la habilitan para imponer a sus propios funcionarios y a los particulares el acatamiento, inclusive por medios punitivos, de una disciplina cuya observancia contribuye a la realización de sus cometidos. Esa potestad es una manifestación del *jus punendi*, por lo que está sometida a los siguientes principios: (i) el principio de legalidad, que se traduce en la existencia de una ley que la regule; es decir, que corresponde sólo al legislador ordinario o extraordinario su

¹⁴⁷Artículos 66 y 67 de la ley 489 de 1998 da una descripción básica de lo que son las Superintendencias y las Unidades administrativas especiales.

definición. (ii) El principio de tipicidad que, si bien no es igual de riguroso al penal, sí obliga al legislador a hacer una descripción de la conducta o del comportamiento que da lugar a la aplicación de la sanción y a determinar expresamente la sanción. (iii) El debido proceso que exige entre otros, la definición de un procedimiento, así sea sumario, que garantice el debido proceso y, en especial, el derecho de defensa, lo que incluye la designación expresa de la autoridad competente para imponer la sanción. (iv) El principio de proporcionalidad que se traduce en que la sanción debe ser proporcional a la falta o infracción administrativa que se busca sancionar. (v) La independencia de la sanción penal; esto significa que la sanción se puede imponer independientemente de si el hecho que da lugar a ella también puede constituir infracción al régimen penal.”

Las características de la potestad sancionatoria según el profesor Laverde (2016:8) son: a) Realiza los principios constitucionales, b) Hace cumplir las obligaciones y cargas que tienen todos los ciudadanos, más aún con relación a los funcionarios públicos, c) Previene a los que infringen la norma administrativa, d) Su sanción no afecta la libertad, e) La decisión no es cosa juzgada y puede someterse a la jurisdicción contenciosa administrativa en virtud del principio de legalidad.

ii) Funciones como autoridad de protección de datos personales

Las entidades que ofician como Autoridad Pública de Control tienen una serie de facultades comunes a las demás autoridades de otros Estados que se encargan de la protección de datos personales. Estas se encuentran en el artículo 21 de la LEPDP y pueden agruparse así: (i) Hacer cumplir el ordenamiento jurídico sobre protección de datos personales(21-a, 21-e y 21-g) o con cooperación internacional(21-j), iniciando para ello investigaciones(Art. 21-b) o vigilando a los responsables o encargados(21-f) e imponiendo sanciones, (ii) Ordenar medidas temporales ante riesgos eventuales(21-c), (iii) Promover el conocimiento de las normas sobre habeas data(21-d), (iv) Llevar el registro y vigilancia de las entidades que tratan datos

personales (21-h), (v) expedir orientaciones y conceptos sobre la aplicación de las normas de protección de datos personales (21-i).

- Cumplimiento del ordenamiento jurídico sobre protección de datos personales: Se manifiesta en la autorización para hacer inspección y vigilancia a las personas encargadas o responsables del tratamiento. Se destaca que la declaración de conformidad de las transferencias internacionales de datos, las órdenes impartidas a los administradores de bases de datos y la solicitud de colaboración a las autoridades de otros estados para detener la afectación de derechos, son aspectos no taxativos de la realización de este deber.
- Facultad de inspección y vigilancia: Establecida en el literal b y f, permite que la SIC pueda hacer cumplir la normativa de la LEPDP. Para ello se le habilitó la facultad de iniciar investigaciones de oficio o recibirlas de las quejas que radican los titulares que creen afectados sus derechos. Para eso la SIC puede solicitar información a los encargados o responsables del tratamiento acerca de las políticas internas de tratamiento de información y los procedimientos técnicos utilizados para tratar datos personales. Más adelante se ampliará sobre las quejas y las investigaciones administrativas de oficio.
- Ordenar medidas de bloqueo temporales¹⁴⁸ para proteger los derechos fundamentales cuando se presume necesario mientras se adopta una decisión definitiva. Esto se realiza a solicitud del titular. Está es una medida cautelar anticipatoria que de manera innovadora se ha establecido para los procedimientos administrativos sancionatorio por violación de las normas de protección de datos personales, esto lo confirma la respuesta dada por la SIC mediante oficio del 16 de Mayo de 2014 que dice:

¹⁴⁸Que en las autoridades de otros países se les llama facultades cautelares (Cerde, 2006: 246), aunque en Colombia no es procedente llamarla así pues no es una facultad concedida como autoridad jurisdiccional sino administrativa.

“El literal c del artículo 21 de la Ley 1581 de 2012 otorga la siguiente función a la Superintendencia de Industria y Comercio, en su calidad de autoridad nacional de protección de datos personales:

“La Superintendencia de Industria y Comercio ejercerá las siguientes funciones: (...) c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva;” (2)

De acuerdo con lo cual, **la única medida cautelar que el ordenamiento jurídico ha previsto para las investigaciones administrativas** con ocasión a una **posible infracción al Régimen General de Protección de Datos Personales** ha sido el bloqueo temporal de los datos.” (Negrilla fuera de texto)

Lo cual genera no pocas problemas la afirmación y el entendimiento, pues dentro de las etapas respectivas no se encuentra el decreto de dicha medida así como también el hecho de que esa medida este asignada a una autoridad administrativa en ejercicio de facultades administrativas y no jurisdiccionales, hace casi que nugatorio los efectos benévolos que se quisieron perseguir a efectos de prevenir la conducta que afecta el derecho del habeas data o a evitar un mayor agravamiento.¹⁴⁹ Sólo los jueces – entiéndase también autoridades administrativas con facultades jurisdiccionales - tienen la facultad de decretar medidas cautelares y dentro de un proceso judicial.¹⁵⁰

¹⁴⁹Sobre la naturaleza jurisdiccional de las medidas cautelares ha dicho la Corte Constitucional en sentencia C-379 de 2004: “(...) puesto que desarrollan el principio de eficacia de la administración de justicia, son un elemento integrante del derecho de todas las personas a acceder a la administración de justicia y contribuyen a la igualdad procesal.” Y los únicos que administran justicia son los jueces de manera prioritaria y los particulares (inciso 4° Art. 119 Constitucional) o autoridades públicas (inciso 3° Art. 119 Constitucional) que se les da facultad jurisdiccional.

¹⁵⁰ “Los jueces, en ejercicio de su función, las deben concretar en cada proceso, de tal manera que aún en las hipótesis en que su atribución para decidir sea amplia, la discrecionalidad jamás pueda constituir arbitrariedad. “ (Sentencia C-379 de 2004)

- Promover el conocimiento de las normas sobre habeas data que implica socializar entre todas las personas las normas sobre régimen de protección de datos personales de manera preventiva y dar conceptos jurídicos sobre su aplicación.
- Llevar el registro de las entidades que tratan datos personales y vigilar para facilitar la labor de control y vigilancia.
- Expedir orientaciones y conceptos sobre la actualización de las normas de protección de datos personales para las entidades administradoras o tratantes de datos personales, acorde a los cambios tecnológicos.

iii) Poder sancionador: Procedimiento administrativo sancionatorio

La manera como ejerce el poder de policía administrativa es a través del procedimiento administrativo, que se desarrolla en unas etapas y trámites pertinentes que permite el respeto de los derechos fundamentales del administrado investigado. Además de ser respetuosos de los derechos también deben ser justos y razonables, con miras a evitar que se contagie del populismo punitivo que asoma en el derecho penal (Laverde, 2016: xxxiv)

El proceso administrativo sancionatorio debe respetar de la dignidad de la persona inmersa en la actuación administrativa, esto se cumple cuando se respetan las formalidades del procedimiento, los principios procesales¹⁵¹ y sustanciales¹⁵² y la efectividad de otros derechos fundamentales del afectado inmersos.

La ley LEPDP remitía el procedimiento administrativo del Código Contencioso Administrativo, sin embargo por virtud de la derogación que hizo el Código de Procedimiento Administrativo y de lo Contencioso Administrativo debe aplicarse los artículos que se hallan en el título 3 de la primera de este Código. Aunque se está de acuerdo con la opinión de la Corte¹⁵³ que debió regularse dentro de la misma ley, e inclusive es más adecuado que este en

¹⁵¹Celeridad, igualdad, moralidad, eficacia, economía, publicidad, juez natural, etc.

¹⁵²Legalidad, presunción de inocencia,.

¹⁵³"No obstante lo anterior, la Corte concuerda con la intervención de la Defensoría del Pueblo, en el sentido que el legislador debe hacer un esfuerzo por regular de forma sistemática y clara los procedimientos sancionatorios, sin necesidad de remisiones que en ocasiones dificultan su aplicación. "

el tipo de ley que exige la Constitución, por tanto se regule como procedimiento administrativo especial de protección de este derecho fundamental así como otros procedimientos administrativos sancionatorios que tienen su propia normativa.

A continuación se exponen los dos instrumentos que usa la Autoridad Pública para iniciar el procedimiento administrativo:

Queja

Respecto a este instrumento se encuentra establecido como uno de los derechos del titular en el literal g) del artículo 8 de la LEPDP. Es desarrollado por el artículo 16 de la misma LEPDP en cuanto a que impone el requisito de reclamo ante el responsable para poder usar la queja ante la SIC.

Este es un requisito para garantizar la economía procesal de la SIC, de tal forma que solo conozca de aquellos casos más que expongan a un riesgo de mayor vulneración del habeas data bajo el criterio de renuencia en el cumplir con lo pedido en la consulta o reclamación.

Indagación preliminar de oficio

Consiste en las averiguaciones previas que realiza la Delegatura de Protección de Datos Personales de la SIC a partir de la información recabada o remitida por los encargados o responsables del tratamiento de datos personales.

En los dos casos anteriores si cree pertinente abrirá el proceso administrativo, notificándole al interesado que queda vinculado a la investigación.

Apertura formal

Posteriormente las etapas subsiguientes se rigen por el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA) en los artículos 47 a 52. El procedimiento administrativo a partir de la apertura formal del mismo pasará a realizarse escrito, por audiencias o por vía electrónica, se formularan los cargos, se recibirán los descargos y se tomará la decisión bajo los criterios de graduación que establece la LEPDP y no el CPACA.

Deberá guiarse por los principios del debido proceso constitucional, entre los cuáles merece destacarse el principio de contradicción, el cual le permite al interesado presentar las pruebas y descargos pertinentes, así como participar a otros interesados¹⁵⁴ es el que hace viable este mecanismo. Adicionalmente como es tramitado en un ente técnico, existe la confianza de que el servidor público que lo lleve tenga los conocimientos y facultades suficientes para impedir una vulneración más agravada del derecho al habeas data.

Por la estructura señalada en el segundo inciso¹⁵⁵ del artículo 47 del CPACA se puede deducir que no está contemplada en ninguna etapa el decreto de medida cautelar del bloqueo temporal, y de decretar dicha medida en la etapa inicial, la de formulación de cargos, la cual creemos que es la más adecuada, está violando el debido proceso administrativo.

iv) Poder de policía administrativa: Registro Nacional de Base de Datos

En la LEPDP se encuentra regulada en el artículo 25 y lo define como “(...)el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.” Tiene la obligación de registrarse en ella las personas que realicen tratamientos automatizados o manuales de

¹⁵⁴El artículo 38-2 del CPACA permite hacerlo, porque el procedimiento administrativo sancionatorio no reguló nada especial al respecto sobre intervención de interesados.

¹⁵⁵“ Concluidas las averiguaciones preliminares, si fuere del caso, formulará cargos mediante acto administrativo en el que señalará, con precisión y claridad, los hechos que lo originan, las personas naturales o jurídicas objeto de la investigación, las disposiciones presuntamente vulneradas y las sanciones o medidas que serian procedentes.”

datos (dentro o fuera del país pero con domicilio legal en territorio nacional o por aplicación de un tratado internacional), cualquiera que sea su naturaleza, de todas las bases de datos que tengan administrando o tratando, según lo establece el ámbito de aplicación del artículo 2 del decreto 886 de 2014.

Pese a que hace parte de las funciones de la Superintendencia de Industria y Comercio llevar el registro nacional de bases de datos (RNBD) se considera que es una herramienta jurídica de protección de datos personales porque permite el ejercicio del control de la información, especialmente del derecho de conocer cuales bases de datos tienen información personal nuestra.¹⁵⁶ En efecto a través del ejercicio de la consulta las personas pueden conocer cuántas bases de datos tienen información personal de ellos, con que finalidad y como la están tratando

Autorregulación

La LEPDP estableció una serie de mecanismos administrativos y organizacionales que son requisitos algunos de procedibilidad para iniciar un procedimiento administrativo ante la SIC por violación de la ley, pero todos en su mayor parte buscan consecuencias jurídicas claras: que se permita el ejercicio de los Derechos ARCO. Para el profesor Nelson Remolina las herramientas jurídicas de la autonomía privada hacen parte de los derechos de los titulares y le permiten “(...) facultades esenciales para controlar la recolección, el almacenamiento, el uso, la circulación, el acceso y la calidad de los datos personales” (Remolina, 2013:225)

Hay otras herramientas jurídicas de protección que hacen parte del proceso de reconocimiento del poder normativo externo diferente al Estado, en efecto estos son las normas corporativas vinculantes y los códigos deontológicos, esto ha producido lo que el profesor Pérez Luño (2006:53) denomina “ampliación de competencias normativas” a poderes

¹⁵⁶ Dice el artículo 4 del decreto 886 de 2014: “Los ciudadanos podrán consultar en el Registro Nacional de Bases de Datos, la información mínima prevista en el artículo 5° del presente decreto con el fin de facilitar el ejercicio de sus derechos a conocer, actualizar, rectificar, suprimir el dato y/o revocar la autorización.”

ciudadanos, sociales, empresariales diferentes del clásico poder estatal, quien no cede su capacidad soberana de producir normas, solamente reafirma lo que ya socialmente estaba reconocido como norma eficaz para una agremiación (códigos deontológicos) o dentro de un sector de comercio mundial o una multinacional con sus filiales(normas corporativas vinculantes).

En Colombia son reconocidos las herramientas de consulta y reclamo ante los encargados y responsables del tratamiento, las políticas de tratamiento de la información y las normas corporativas vinculantes a nivel contractual, que imponen obligaciones frente a los titulares de datos personales.

a. Consulta: Derecho de petición para obtener datos personales

Está reconocido en el art. 14 de la LEPDP y en el art.21 del decreto 1377 de 2013. En conjunto ambas disposiciones normativas permiten afirmar que la consulta es un derecho de petición para obtener información acerca de los datos personales que se tienen de nosotros y la manera en que se están tratando. Al respecto ha dicho la Corte sobre la consulta como modalidad del derecho de petición:

“Es precisamente esta regulación la que hace el artículo 14, al estipular que los responsables y/o encargados del tratamiento de datos, en este caso los privados, deben atender en los precisos términos las consultas que eleven ante ellos los titulares del derecho al habeas data, como una forma de hacer exigibles el derecho consagrado en el literal a) del artículo 8 del proyecto en revisión, específicamente el de conocer.

En este orden de ideas, el derecho de petición que se regula en la norma objeto de análisis se convierte en un instrumento con el que cuenta el titular del dato para hacer exigible o realizable el derecho autónomo de habeas data.”

La respuesta dada al titular del dato o a un representante (causahabiente, mandatario, estipulante a favor)¹⁵⁷ de este debe ser satisfecha lo que implica tres aspectos, en el primero “(...) debe ser de fondo, es decir, no puede evadirse el objeto de la petición, **(ii)** que de forma completa y clara se respondan a los interrogantes planteados por el solicitante, **(iii)** oportuna, asunto que obliga a respetar los términos fijados en la norma acusada.”

En el caso de no ser competente para responder a la petición debe darle traslado a quien si lo sea, es decir, si llega una consulta al responsable del tratamiento y este no conoce específicamente la manera en están siendo tratados los datos personales de manera técnica o qué medidas de seguridad se encuentran implementadas debe remitirla al encargado del tratamiento.

El encargado o el responsable deben establecer la manera más ágil y sencilla en que puede ser ejercido esta herramienta. Esto viene condicionado a que pueda ser ejercido durante dos situaciones, primordialmente gratuitas: i) que pueda ejercerse una vez al mes y ii) Cuando existan cambios en las Políticas de Tratamiento de Datos Personales.

Cuando están fuera de estos supuestos de hecho, el encargado debe fijar un procedimiento para que pague una suma de dinero, esta cantidad solo podrá ser por gastos administrativos de certificación, de envío del documento o de reproducción. Frente a lo que opina el profesor Nelson Remolina (2013:233) sobre la injusticia del cobro por consulta superior a un mes¹⁵⁸, el gobierno en ejercicio de su facultad reglamentaria estableció los casos en que procede, adicionalmente se cree que la afirmación de que son suministrados gratuitamente por el titular del dato personal oculta el hecho de que en algunas ocasiones recibe un beneficio económico o social por hacerlo, que es en este punto incalculable monetariamente, pero lo recibe.

¹⁵⁷Artículo 20, decreto 1377 de 2013.

¹⁵⁸Dice el profesor Nelson Remolina (2013:233): “Ojalá no nos equivoquemos, pero con esta limitación ilegal a la gratuidad, el Decreto 1377 creó otro nicho de negocio en contra del bolsillo de los titulares. El lucro de algunas organizaciones proviene del ejercicio de los derechos que hacen parte del núcleo fundamental del derecho al hábeas data”

b. Reclamo

El reclamo se encuentra regulado en el artículo 15 de la LEPDP y permite el ejercicio de cualquiera de los derechos de rectificación, cancelación, oposición y revocación de la autorización.

La Corte Constitucional en sentencia C-748 de 2011 determinó tres aspectos frente a los cuales el titular del dato puede reclamar: i) Cuando no se cumplen los principios, derechos y garantías constitucionales diferentes al habeas data, siempre que haya sido sancionada por la SIC y ii) Por solicitud voluntaria del titular del dato respecto a la existencia presunta de un incumplimiento en sus derecho o la carencia actual de vínculo jurídico que le obligue a tener almacenada su información iii) Cuando haya intereses constitucionales relacionados con su libertad u otros derechos fundamentales que obligan a detener el tratamiento de datos para los fines autorizados.

El titular del dato personal puede con el reclamo hacer revocatoria de la autorización de manera total o parcial, para actualizar o rectificar su información personal o para oponerse a la manera como están tratando su información personal que incumple con los deberes del encargado o afecta sus derechos fundamentales. El trámite debe durar máximo 15 días hábiles, que se extienden por una sola vez en 8 días más, durante los cuales se debe poner la reseña que diga del dato personal “reclamación en trámite” con el motivo

A continuación se establece la tipología de reclamo que estableció la SIC para organizar las remisiones semestrales, que deben hacer los operadores de información (según la ley 1266 de 2008 aplicable a datos financieros, comerciales y crediticios), que pueden entenderse como los encargados del tratamiento en términos de la ley LEPDP, para efectos ilustrativos:

**TIPOLOGÍA DE RECLAMOS QUE DEBEN REPORTAR LOS OPERADORES DE
INFORMACIÓN SEGÚN LA LEY 1266 DE 2008**

Tipología	Subtipología	Código
Actualizar la información	No actualiza la información	01
	No reporta oportunamente la información	02
	Reporta la información incompleta o parcial	03
	No incluye las respectivas leyendas	04
	Inconformidad con la permanencia de la información negativa	05
Rectificar la información	No rectificación de la información errónea	06
	Inexistencia de la obligación reportada o negación de la relación contractual	07
	No contar con los documentos soporte de la obligación	08
	No contar con la autorización previa y expresa del titular para reportar información	09
	No certificar semestralmente al operado que la información suministrada cuenta con la respectiva autorización del titular	10
	No remitir la comunicación previa al soporte	11
Conocer la información	Negación de acceso a la información	12
	No atender las peticiones y reclamos presentados por los titulares de fondo y oportunamente	13
	No adoptar las medidas de seguridad adecuadas sobre la información obtenida en las bases de datos de los operadores	14
	Utilizar la información para una finalidad diferente a aquella para la cual fue entregada	15
	Consulta de información no autorizada por el titular, cuando esta sea requerida	16

	No contar con medidas adecuadas de seguridad	17
	No informar al titular sobre la utilización que se le está dando a su información	18
	No informar al titular la finalidad de la recolección de la información	19
	No guardar reserva sobre la información	20

Fuente: SIC (2012) Resolución N°76434 DE 2012

c. Normas corporativas vinculantes

Las prácticas empresariales vigentes en esta economía globalizada no pueden ser un instrumento para ignorar los derechos fundamentales y la dignidad humana de las personas cuyas datos son llevados entre varios países. Las empresas también reconocen que utilizar estándares en el manejo de los datos personales les va a ayudar en una imagen más positiva y una mayor seguridad en sus relaciones de negocios. Esto aplica fundamentalmente a las empresas que se ubican en varios países.

Son un conjunto de políticas de tratamiento de los datos personales que se formalizan como un contrato vinculante entre un grupo empresarial que requiere una transferencia de datos personales a un país que no tiene la certificación de nivel adecuado de protección de datos personales según los estándares internacionales. Permiten que una persona jurídica, generalmente la cabeza del grupo, garantice la vinculatoriedad de sus políticas de tratamiento para las filiales localizadas en otros países que fungen como encargados del tratamiento o como responsables del tratamiento.

El fenómeno social que hizo necesaria estos acuerdos privados se debe a la necesidad garantizar la normativa de protección de datos en las transferencias internacionales de datos ante el fenómeno de la globalización de la transferencia y recolección internacional de datos personales de una empresa a otra que, amparada en la ubicación de su domicilio en otro país, hizo inexigible la aplicación de sus normas a datos provenientes del primer país.

Las normas corporativas vinculantes son un mecanismo de autorregulación para aceptar las normas jurídicas de un país sobre tratamiento de datos personales. Al ser un contrato internacional, es aplicable el principio de la *lex loci contractus*¹⁵⁹¹⁶⁰, que permite seleccionar un ordenamiento jurídico base, sobre el cual los contratantes se van a regir para la ejecución del contrato. Al respecto sobre la *Lex Contractus* dice el profesor Javier García(2010:67):“Por un lado, faculta a los contratantes a crear obligaciones convencionales a través de una PL-Law[poder legislativo de los contratantes];por otro lado, complementa las disposiciones convencionales al establecer al menos la norma *pacta sunt servanda*”

Así las cosas las normas corporativas vinculantes incluyen una pluralidad de partes en el contrato de un lado responsable del tratamiento y su grupo empresarial, que recolecta los datos personales de sus filiales en varios países, del otro el encargado y su grupo empresarial, que se encarga de las labores de tratamiento. Incluso puede afirmarse que sería plurilateral de un lado, el del encargado del tratamiento. El punto es que el titular tenga garantías y transparencia para dar conscientemente su autorización de quienes y bajo qué condiciones se tratarán y en qué países, así como las normas que aplican y las obligaciones de indemnización en caso de daño.

Se permite el flujo de información que exige la globalización sin perjudicar los derechos fundamentales debido a que un responsable del tratamiento domiciliado en un país, que exige un nivel de protección igual o superior al de su país para transferencias a otro, tenga la confianza de remitir datos personales a un encargado del tratamiento domiciliado en un país sin una norma o con una norma no valorada como de nivel adecuado para la protección, pero que en virtud de las normas corporativas vinculantes del grupo empresarial al que pertenece,

¹⁵⁹Este hace parte de la *lex contractus* que define así García (2010:67): “La *lex contractus* integra por el consensus de los contratantes sustentado en un *grundlegung* (*lex contractus*= *grundlegund* + *consensus*)”, esto es así porque para que pueda darse la aplicación se tienen en cuenta el ordenamiento jurídico que permite la autonomía a las partes para elegir de consenso la norma aplicable. En el mismo sentido se pronuncia el profesor Javier Carrascosa(2013:25): “La facultad de elegir la ley del contrato deriva de la ley, y en concreto, de la norma de conflicto (...) permite a las partes elegir la ley que regula su contrato(*lex contractus*)

¹⁶⁰Sobre este tema se han establecido para América la Convención Interamericana sobre el derecho aplicable a los contratos internacionales, que permite la libre elección en su artículo 7. Colombia no lo ha ratificado. Para la Unión Europea se tiene el Reglamento de Roma I (Reglamento CE/593/2008, sobre la ley aplicable a las obligaciones contractuales que afecten a más de un país miembro y el reglamento CE/864/2007 para obligaciones extracontractuales.

que estableció su casa matriz, se garantiza el cumplimiento de la seguridad en la información. Esto no sería posible con los contratos estándar o cláusulas de transferencia internacional de datos hacia terceros países, pues estos son válidos para la transferencia uno a uno, no entran en flujo internacional constante de datos personales, son vinculantes con efectos entre partes pues no los reconoce la autoridad pública competente.

Las dos maneras en que pueda darse la aprobación de las normas corporativas vinculantes por parte de la autoridad pública de protección de datos personales son: a) recibir la certificación de un auditor que garantiza el cumplimiento de la normativa nacional en el tratamiento de datos personales que se implementa por medio de las NCV, se les conoce como sellos de certificación, b) se conceda validez al dictamen de aprobación de las NCV que emitió una autoridad del país de domicilio legal de la entidad que desea ver válidas sus normas, en virtud de algún tratado o principio de colaboración entre ambos países y autoridades. c) que la misma autoridad pública de control examine las NCV y decida que cumplen con las normas de protección de datos personales del país que representa.

d. Políticas de tratamiento de los datos personales

Estas políticas de tratamiento implican el cumplimiento de unos requisitos mínimos de tratamiento e identificación del encargado frente al titular. A nuestro concepto, implican una declaración unilateral de voluntad del encargado para comprometerse frente al titular, de manera transparente, sobre los fines, tiempo y forma en que tratará la información que de él recolecte.

Es requisito indispensable esta herramienta jurídica para que se pueda dar la autorización de tratamiento de los datos personales, se comunica mediante el “aviso de privacidad”¹⁶¹. Implica el reconocimiento inicial del derecho al Habeas Data porque es la

¹⁶¹ Se define como una forma de comunicar a través de “(...) cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular (...)” “(...) sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales.” (Decreto 1377 de 2013, artículo 17 y 14 respectivamente)

facultad que denota el ejercicio de la autodeterminación informativa o libertad informática para la recolección de información. “Esa libertad es la decisión voluntaria e informada del titular de permitir que otras personas recolecten, almacenen, usen, envíen o realicen cualquier actividad con sus datos personales” (Remolina, 2013:228) Como bien la recolección hace parte del núcleo esencial, que para realizarse se requiere de la autorización, aspecto que se da frente a un documento específico que se denomina políticas de tratamiento de datos personales.

En esta herramienta jurídica se conservan los siguientes aspectos: a) prueba de la autorización otorgada al responsable del tratamiento, b) conservación de la autorización del titular, c) Políticas de tratamiento de datos personales que ha consentido d) Usos posibles de los datos personales, e) Encargados de realizar el tratamiento a los cuales ha permitido el acceso y se les suministrará en algún momento los datos, f) los derechos del titular del dato personal, g) las obligaciones de los encargados y responsables del tratamiento, h) la forma de ejercer los derechos del titular y g) vigencia de la política de tratamiento

Los responsables del tratamiento de la información personal tienen la obligación de redactar las políticas antes de iniciar el tratamiento, velar porque se cumplan adecuadamente por parte de los encargados del tratamiento.

Derechos del Habeas Data que garantizan los mecanismos para la protección de datos
personales en Colombia

*“La necesidad de disciplinar
la informática es una exigencia
de la tutela de la libertad individual.”*
Matilde Zabala,
Derecho a la intimidad

Los derechos fundamentales deben regularse mediante una ley estatutaria, eso es lo que señala la Constitución colombiana, por su importancia reconocida no pueden quedar sometidos a los vaivenes normativos que se ciernen sobre las normas ordinarias que expide el legislador.

Por esta razón deben regularse los aspectos más importantes para la tutela de los derechos, que la Corte, a partir de “núcleo esencial” entiende compuesto por “(...) el contenido básico que no puede ser limitado por las mayorías políticas ni desconocido en ningún caso, ni siquiera cuando un derecho fundamental colisiona con otro de la misma naturaleza o con otro principio constitucional” y “(...) un contenido adyacente objeto de regulación”.

Los aspectos que debe regular en el contenido adyacente son: límites, excepciones y prohibiciones de alcance general, los principios básicos para su ejercicio, los derechos de los titulares y las obligaciones de los sujetos pasivos. La presente sección se concentrará en el objeto protegido por la constitución del derecho de habeas data, su estructura de derecho fundamental y los derechos protegidos por las herramientas jurídicas, tres aspectos importantes para desarrollar en la siguiente sección el análisis del nivel de protección de las herramientas jurídicas

Objeto de protección constitucional del derecho de protección de datos personales

“Bajo las condiciones del tratamiento automático
Ningún dato es *insignificante*”

Ernesto Benda

Dignidad humana y derechos de la personalidad

Los derechos fundamentales son reconocidos a distintos niveles de positivación (Pérez Luño, 2005:67-110): nivel internacional (incorporado posteriormente al ordenamiento jurídico estatal, nivel constitucional, nivel legal, nivel ejecutivo y nivel judicial.

En Colombia el derecho a la protección de datos personales, se enmarcó inicialmente por intimidad, que está positivizado a 3 niveles: a nivel internacional por la Convención Americana de los Derechos Humanos, a nivel constitucional en el artículo 15 de la Carta Magna vigente y a nivel legal con la ley estatutaria 1581 de protección de datos personales. Sin embargo esta ley regula el desarrollo legal del derecho constitucional, haciendo una transcripción del artículo 15 constitucional, por lo cual se hace necesario repasar la jurisprudencia hito acerca del desarrollo del contenido del derecho fundamental del Habeas Data, el objeto de protección, la estructura del derecho fundamental, los derechos protegidos y los procedimientos establecidos para exigirlos.

En una primera etapa se configura el Habeas Data¹⁶² como una garantía de la intimidad¹⁶³, la Corte en esta primera etapa dice que es una garantía o un derecho de obtener el conocimiento acerca del uso que se realiza de nuestros datos personales para que no afecten nuestra esfera privada y se produzcan injerencias indeseadas. En sentencia T-444 de 1992 afirma que “(...)implica la posibilidad de ser informado acerca de los datos registrados sobre

¹⁶² “Como se advierte de la lectura del artículo 15, el derecho a la intimidad comprende varias dimensiones de la vida privada. En este caso concreto, sin embargo, se trata sólo de una de tales dimensiones: el habeas data, razón por la cual el análisis se centrará en este tema.” Sentencia T-444 de 1992 MP Alejandro Martínez Caballero. La sentencia T-340 de 1993 coincide en la idea esencial acerca del Habeas Data como parte del derecho a la intimidad. Se confirma lo dicho de manera inicial en sentencia T-008 de 1993.

¹⁶³ Así explica la corte: “(...)de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir” (Sentencia C-748 de 2011 MP Jorge Pretelt Chaljub)

sí mismo y la facultad de corregirlos. Con este derecho se pretende proteger la intimidad de las personas ante la creciente utilización de información personal (...). Lo importante es que las personas no pierdan el control sobre la propia información, así como sobre su uso.”; en esta sentencia se destacan dos ideas que propuso la Corte acerca de este derecho: i) previene la pérdida de control de la información personal y ii) Obligación de cumplir con unos principios de administración de datos personales, el germen del derecho al debido tratamiento de datos personales. En sentencia SU-528 de 1993 afirma que es un “(...) instrumento de defensa de la dignidad humana y de los enunciados derechos de toda persona en lo que respecta a la exactitud de las informaciones que en torno a ella se hayan conocido y se divulguen.”.

Se entendió que el indebido tratamiento de datos personales vulneraba el derecho a la intimidad porque se tenía acceso constante al ámbito de la vida privada a través de la recopilación de información, que posteriormente era usada para proferir juicios acerca de la persona sin que esta lo supiera, de esta manera se perturbaba ese espacio reservado solamente a uno, a pesar de que se hubiese dado el permiso de acceder a la información, porque las consecuencias de dar dicho permiso se proyectaron más allá de lo que cada persona piensa al entregarla. La Corte Constitucional colombiana le llama a la capacidad de las nuevas tecnologías poder informático¹⁶⁴ que genera “la posibilidad de acumular informaciones en cantidad ilimitada, de confrontarlas y agregarlas entre sí, de hacerle un seguimiento en una memoria indefectible, de objetivizarlas y transmitir las como mercancía en forma de cintas, rollos o discos magnéticos.(....) Como puede advertirse, el abuso o la negligencia en el ejercicio de este enorme poder, apareja un serio riesgo, entre otros, para los derechos fundamentales a la personalidad, a la identidad, a la igualdad, a la intimidad, a la honra, al buen nombre o al debido proceso del sujeto concernido. “ (Corte Constitucional, Sentencia T-414 de 1992.)

Por un breve lapso de tiempo y en forma paralela se afirma del Habeas Data que permite el ejercicio de una libertad informática¹⁶⁵ respecto a los datos personales, a su uso,

¹⁶⁴En Sentencia T-307 de 1999 MP Eduardo Cifuentes Muñoz sigue la línea jurisprudencia de considerar a las nuevas tecnologías como habilitantes de un poder grande sobre las personas.

¹⁶⁵La sentencia T-022 de 1992 lo considera como una facultad de la persona porque “(...) su fundamento último en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de su personalidad y en homenaje justiciero a su dignidad. Dentro de ese refugio jurídicamente amurallado que lo

rectificación, difusión y transmisión, que dicha libertad incide en el desarrollo de la personalidad.

En una segunda etapa que inicia a partir de 1995¹⁶⁶, la Corte Constitucional define el Habeas Data como un “(...) un derecho fundamental autónomo que tiene la función primordial de equilibrar el poder entre el sujeto concernido por el dato y aquel que tiene la capacidad de recolectarlo, almacenarlo, usarlo y transmitirlo.” (en sentencia T-307 de 1999), así como garantizar la libertad económica y la libertad en general (en sentencia SU-082 y SU-089 de 1995). La justificación se fundamenta en que es necesaria una supervisión al poder informático ante la importancia que adquiere el uso de la información y su incidencia en las libertades personales¹⁶⁷; la Corte en esta etapa le llama derecho a la autodeterminación informática al Habeas Data, concluye que es un derecho fundamental y autónomo.

En esta etapa aún siguen bastante influenciados por la idea del habeas data como garantía de la intimidad personal y familiar, del buen nombre y de la honra¹⁶⁸, por ello cada persona es la autorizada para dar el permiso de acceso a aquello que no es conocido públicamente, así es visto el análisis en las sentencias emitidas antes del año 1995¹⁶⁹. A partir de este año comienza el progresivo desligamiento del derecho al habeas data de la intimidad, así en sentencia T-552 de 1997 afirmó que es totalmente independiente y diferenciado¹⁷⁰

(cont. Cita 165) protege, el sujeto puede actuar como a bien lo tenga. De ahí que las divulgaciones o investigaciones que penetren tal muro sólo podrán ocurrir por voluntad o aquiescencia del sujeto o cuando un verdadero interés general legitime la injerencia.”

¹⁶⁶Sentencia T-097 de 1995 y T-119 de 1995

¹⁶⁷ “Según esta línea, el habeas data tiene su fundamento último “(...) en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad” (Sentencia C-728 de 2011 MP Jorge Pretelt Chaljub)

¹⁶⁸La sentencia T-814 de 2003 en la cual la Corte afirma: “Por otra parte, dentro del espacio privado, la intimidad protege a los individuos frente a interferencias de diversa índole. Esta protección no sólo se logra garantizando los derechos sobre la propiedad individual. Esta protección implica también la facultad de actuar dentro de un espacio privado sin interferencias visuales, sonoras u olfativas. Ello no significa que en aras de proteger la intimidad dentro de un espacio privado deban anularse las libertades individuales de los demás. Por el contrario, la vida en comunidad supone la necesidad de armonizar la intimidad con otras libertades y derechos individuales, de tal modo que se sacrifique lo menos posible el contenido de cada uno de ellos. Por tal motivo, al sopesar la intimidad frente a otros derechos y libertades, es necesario tener en cuenta el grado de invasión de la esfera privada.”

¹⁶⁹ Por ejemplo, las sentencias T-110 de 1993, T-157 y T-164 ambas de 1994.

porque se enfoca en proteger la adecuada administración de datos personales a través de 3 facultades: conocer, actualizar y rectificar la información retomadas de sentencias anteriores.

A partir del año 2000 se abre la etapa del Habeas Data como un derecho independiente que denomina de *protección de datos personales*. En esta tercera etapa se le reconoce en principio al Habeas Data la naturaleza de derecho fundamental autónomo¹⁷¹ (sentencia T-578 de 2000) compuesto por la autodeterminación informática y la libertad informática, posteriormente en la sentencia T-729 de 2002 se hace énfasis en que el Habeas Data es el derecho a la autodeterminación informática a través del ejercicio de las facultades de acceso, inclusión, exclusión, corrección y adición así como también a la supervisión para limitar el uso de los datos personales a través de lo que denomina principios para la administración de datos personales, en esta sentencia hace un acopio sistemático de los principios que estaban enunciados de manera dispersa a lo largo de la sentencia.

En sentencia posterior, la T-814 de 2003, afina el ámbito de operatividad del habeas data según el aspecto que pretende tutelarse jurídicamente: i. aspectos concernientes a la vida íntima que no desean ver publicados o ii. La incidencia de los externos sobre ella a través del tratamiento de datos personales, dado que a su juicio la línea público/privado se ha hecho borrosa. No olvida remarcar que el habeas data protege la intimidad personal de los individuos de intromisiones en la capacidad de actuar¹⁷².

¹⁷⁰“El derecho al habeas data es, entonces, un derecho claramente diferenciado del derecho a la intimidad, cuyo núcleo esencial está integrado por el derecho a la autodeterminación informativa que implica, como lo reconoce el artículo 15 de la Carta Fundamental, la facultad que tienen todas las personas de “conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.”

¹⁷¹ La Corte en Sentencia T-527 de 2000 afirma lo siguiente: “En relación con la protección constitucional del artículo 15 de la Carta, ha señalado esta Corporación, múltiples veces, que el Habeas Data es el derecho que tienen todas las personas a “conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas”.

¹⁷² “Los derechos mediante los cuales se protege la privacidad de individuos y familias **operan de manera distinta, dependiendo de si sólo se pretende proteger frente a la intromisión de terceros, o si además se quiere impedir la exteriorización o difusión no autorizadas de aspectos de su vida.** Aun cuando en los dos casos se protege la libertad individual, en el primero, el ámbito de protección tiene un carácter general, como facultad de actuar en privado sin la interferencia de terceros. En el segundo, **la protección se extiende a un campo específico de la libertad: la autodeterminación informativa.** Como se dijo anteriormente, en el presente caso no se está divulgando información acerca de la vida íntima de la demandante o de su familia. Resta saber si se está interfiriendo en su capacidad de actuar dentro de un espacio privado, reservado al individuo y a su familia.”(Negrilla fuera de texto, ver Sentencia T-814 de 2003, MP Rodrigo Escobar Gil)

En este punto para comprender cuál es el objeto de protección constitucional del derecho al habeas data debemos realizar esta operación analítica de despojo de elementos subjetivos, lo que implica “prescindir del titular del derecho fundamental (el habilitado), del destinatario del derecho (el obligado) y de la modalidad objeto del derecho)” (Julio, 2000:70).

A partir de la jurisprudencia de la Corte Constitucional, se considera que el objeto de protección constitucional del derecho de Habeas Data o protección de datos personales consiste en **el control de los usos de la información¹⁷³ que concierne a cada una de las personas¹⁷⁴, a través de unas precisas facultades que permite supervisar el tratamiento idóneo**, entendido este, como aquel que no vulnere derechos conexos como la intimidad, el buen nombre, la honra, el honor, la imagen; **el control y la limitación del tratamiento de datos personales sólo puede ser idóneo si se cumplen con los principios que fija en su jurisprudencia para el tratamiento y la administración de datos personales¹⁷⁵.**

¹⁷³ Dada la proyección social de nuestros actos siempre habrá información de otros entrando y de cada uno saliendo, por lo cual a primera vista existe una colisión de derechos: información e intimidad. Pero la Corte en sentencia T-814 de 2003 lo resuelve sabiamente al decir que debe existir un espacio sin interferencias lo menos posible, al cual entra quienes decide la persona, pero no es el único criterio para definir intimidad: La intimidad personal y familiar no sólo protege la capacidad de autodeterminación individual frente a amenazas físicas sobre un espacio privado. Esta protección se extiende a diferentes ámbitos en los cuales las personas desarrollan ciertas actividades, con la esperanza de no tener interferencias de las demás personas. En efecto, el artículo 15 de la Carta protege la privacidad de las comunicaciones interpersonales, de la correspondencia, y de los libros de comercio. En todos estos casos, el ámbito de protección de la intimidad se extiende más allá del concepto de espacio en sentido estricto. En esa medida, aun cuando el espacio dentro del cual se desarrolla una determinada conducta es un criterio importante para establecer si está dentro del ámbito de protección de la intimidad, no es el único parámetro.

¹⁷⁴ Dentro de una concepción *pro homine*, que le reconoce su capacidad de configuración de su propia existencia, en ejercicio de su libertad jurídica. Así lo afirma la Corte Constitucional en Sentencia T-814 de 2003: “En uno y otro caso, todo el mecanismo de persuasión está estructurado sobre una intromisión, “una molestia” de la vida privada que los individuos llevan a cabo al interior de su hogar, para obtener de ellos una cierta conducta. Recurrir a este tipo de instrumentos, invadiendo incluso la privacidad de su hogar, supone una concepción en exceso determinista de la conducta humana. Según esta concepción, los individuos son incapaces de adquirir un verdadero sentido de responsabilidad frente a sus obligaciones, si el Estado o la sociedad no los están presionando permanentemente aun dentro de su hogar. Esta concepción resulta completamente contraria a la filosofía que inspira la Constitución, basada en la dignidad humana, como capacidad del individuo para elegir, y asumir los compromisos y responsabilidades con fundamento en su libre elección.”

¹⁷⁵ Estos principios fijan el ámbito de operatividad del proceso de administración o tratamiento de datos personales dentro del marco constitucional “(...) con el fin de garantizar la armonía en el ejercicio de los derechos fundamentales de las administradoras, de los usuarios y de los titulares de los datos.” (Sentencia T-729 de 2002)

Estructura del derecho fundamental a la protección de datos personales según su desarrollo legal

En el constitucionalismo actual el papel de la ley¹⁷⁶ ha sido desplazado de manera evidente en su superioridad por la Constitución, quien, entre otros aspectos vinculantes, le pone los derroteros básicos por los cuales debe desarrollar normas el legislador. Esto no significa que simplemente el legislador subsuma los enunciados constitucionales a aspectos más concretos, más adecuado,¹⁷⁷ sino que de acuerdo a las necesidades políticas y sociales puede producir normas, que respondan a estas y al mismo tiempo estén de acuerdo a las aspiraciones constitucionales-axiológicas y respete los derechos constitucionales.

Dentro del ejercicio de la facultad legislativo por parte del Congreso de la República de Colombia que le ha sido asignada se encuentran varias competencias normativas según el objeto de la ley: si son el plan de desarrollo o de presupuesto, si regulan mecanismos de participación ciudadana, si incorporan tratados internacionales al ordenamiento jurídico. Esto se denomina reserva de ley, es una técnica por la cual determinadas materias deben ser reguladas según la ley (reserva general) y en concreto por un tipo de ley específica (reserva especial); la ley estatutaria se incluye dentro de esta reserva legal.

Las leyes estatutarias (Art. 152 Constitución colombiana de 1991) son una clase de ley que requiere un procedimiento más estricto para su aprobación, debido a que toca materias muy sensibles e importantes del ordenamiento constitucional. Las materias que se encuentran los derechos y deberes fundamentales de las personas y los procedimientos y recursos para su protección; la administración de justicia; la organización y régimen de partidos y movimientos

¹⁷⁶La Corte Constitucional dice al respecto que el Congreso tiene una competencia normativa general cuando afirma que “ (...)tiene la potestad genérica de desarrollar la Constitución y expedir las reglas de Derecho es el Congreso, pues a este le corresponde “hacer las leyes” (...) No es legítimo considerar que si el Congreso expide una ley que no encaja dentro de las atribuciones específicas del art.150 superior (...) es, (...) inconstitucional, ya que ello implicaría desconocer que en el constitucionalismo colombiano la cláusula general de competencia está radicada en el Congreso” (Sentencia C-527 de 1994)

¹⁷⁷Al respecto Sierra Porto (1998:195) está en contra de que se equipare la relación Constitución-Ley con la de Ley-Reglamento, porque que la Constitución da un margen de maniobra a diversas alternativas políticas, en favor del principio democrático y del pluralismo político que impere en el Congreso; en caso que la Administración actúa con sus reglamentos en cumplimiento de las normas.

políticos, estatuto de oposición y funciones electorales; instituciones y mecanismos de participación ciudadana; estados de excepción.

Los derechos fundamentales requieren de su desarrollo legal en cuanto a las condiciones de ejercicio y las maneras en que puede protegerse, “(...) le corresponde la función de “hacer más realidad los derechos fundamentales (...) actualiza el significado (...) y además concreta los medios que los garantizan” (Sierra Porto, 1998:197). Por ser un derecho fundamental según el artículo 15 de la Constitución colombiana, el habeas data debe regularse por medio de ley estatutaria. Esto en aplicación del principio de reserva que define Sierra Porto (1998:58) como la exigencia de desarrollar o regular determinadas materias a través de un tipo de ley específica, se entiende que incluye también el procedimiento para su aprobación.

La Corte ha afirmado que la ley estatutaria en cuanto a los derechos fundamentales debe regular dos aspectos¹⁷⁸: (i) los elementos esenciales estructurales de los derechos fundamentales, aquello correspondiente al núcleo esencial de ellos, según la teoría adoptada por este tribunal constitucional; y (ii) los mecanismos para su protección, conservando así la efectividad de estos. Los aspectos más detallados del ejercicio de los derechos fundamentales, de cada uno deben. “En materia de derechos fundamentales debe efectuarse ‘una interpretación restrictiva de la reserva de ley estatutaria (...) porque ello conduciría a una petrificación del ordenamiento jurídico’”. (Sentencia C-145 de 1994 MP Alejandro Martínez Caballero)

La Corte Constitucional en múltiples sentencias de tutela configuró el “habeas data” como un derecho a la autodeterminación informática, pero con íntima conexidad a los derechos a la intimidad, del que se desprende, los derechos al buen nombre, a la honra y a la imagen. (Ver considerando 15 de la sentencia T-307 de 1999 MP Eduardo Cifuentes Muñoz). Estos derechos mencionados tienen el carácter de fundamentales, por ello su regulación legal

¹⁷⁸La Corte Constitucional para definir *los elementos estructurales esenciales* se ha valido de la teoría del núcleo esencial que afirma de los derechos que tienen un centro rígido que no puede ceder cuando choca con otros derechos y principios constitucionales y alrededor un contenido desarrollado mediante la reserva de ley estatutaria. Aspectos como el ejercicio de los derechos, las obligaciones específicas de los sujetos pasivos, los principios que guían su aplicación y los mecanismos de protección se encuentran generalmente en este tipo de ley.

debe hacerse mediante una ley estatutaria un tipo especial de ley establecida en los artículos 152 y 153 de la Constitución colombiana.

En nuestro ordenamiento jurídico existen dos leyes estatutarias vigentes, una de carácter general (Ley N°1581 de 2012) que se debe aplicar para la mayor parte de los datos personales que no entran en la excepción del artículo 2° de la misma y otra de carácter específica (ley N°1266 de 2008) aplicable a los datos personales de tipo comercial, crediticio y financiero.

En sentencia SU-082 de 1995 la Corte Constitucional definió la estructura del derecho fundamental del habeas data, o como en ese entonces denominó derecho a la autodeterminación informática. En esa exposición se percibe que tiene la estructura de un derecho a algo, específicamente de un derecho a la *no afectación de propiedades y situaciones*:

“El sujeto activo del derecho a la autodeterminación informática es toda persona, física o jurídica, cuyos datos personales sean susceptibles de tratamiento automatizado.

El sujeto pasivo es toda persona física o jurídica que utilice sistemas informáticos para la conservación, uso y circulación de datos personales. En la materia de qué trata esta sentencia, tales datos deberán referirse a la capacidad económica de la persona, y, concretamente, a la manera como ella atiende sus obligaciones económicas para con las instituciones de crédito.

El contenido del habeas data se manifiesta por tres facultades concretas que el citado artículo 15 reconoce a la persona a la cual se refieren los datos recogidos o almacenados:

- a) El derecho a conocer las informaciones que a ella se refieren;
 - b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos;
 - c) El derecho a rectificar las informaciones que no correspondan a la verdad.
- (...)

Se advierte, finalmente, que el habeas data tiene que ver, además, con la manera como se manejen los datos. Al respecto, el inciso 2º, del artículo 15 dispone:

“En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.”

En consecuencia, los datos conseguidos, por ejemplo, por medios ilícitos no pueden hacer parte de los bancos de datos y tampoco pueden circular. Obsérvese la referencia especial que la norma hace a la libertad, no sólo económica sino en todos los órdenes. Por esto, con razón se ha dicho que la libertad, referida no sólo al aspecto económico, hace parte del núcleo esencial del habeas data.

Contenido del derecho fundamental del habeas data

El contenido del derecho fundamental de habeas data se compone de dos aspectos: objetivo y subjetivo. Como aspecto objetivo se tienen el conjunto de normas, herramientas e instituciones encargados de hacer cumplir el el derecho efectivamente, la manera primordial de hacerlo es verificando el cumplimiento de los principios de administración de datos personales. Las normas establecen las pautas vinculantes para el desarrollo del derecho fundamental, las herramientas jurídicas se encargan de prevenir u detener una afectación al derecho fundamental y las instituciones desde el conjunto de competencias que tienen se encargan de supervisar el cumplimiento de las normas de dos formas: i) orientando la aplicación adecuada de ellas y ii) imponiendo sanciones por el incumplimiento y condenas judiciales que indemnicen la lesión del derecho fundamental.

En el aspecto subjetivo se tienen el conjunto de sujetos intervinientes en la relación jurídica, los derechos concedidos y las obligaciones que imponen. La principal de ellas es que sea realizado un tratamiento de datos personales de forma debida. Lo que se entiende por “tratamiento de datos personales de forma debida” consiste en cumplir con todos los principios de administración de manera imparcial y transparente, sin intención de con ello

perjudicar al titular en otros derechos fundamentales, por ejemplo obteniendo el consentimiento de manera engañosa para publicar fotos íntimas que no son de interés para el público, más allá de un morboso interés a costa del honor de otro, lo que puede perjudicar su buen nombre y propiamente el honor

Adicionalmente el énfasis de este derecho fundamental consiste en ser una garantía instrumental de otros derechos. Por esta razón la Corte Constitucional enfatizó en la sentencia C-748 de 2011 la importancia de contar no sólo con el aspecto subjetivo sino también reforzar el aspecto objetivo, en especial la institucionalidad y las herramientas jurídicas suficientes para garantizar que puedan disputarse los derechos. Al respecto dijo la Corte:

“En ese sentido, es claro que la protección de los datos personales requiere no solo de una regulación que consagre los principios que rigen el tratamiento del dato, los derechos de su titular, los deberes y responsabilidades de los sujetos que intervienen en su tratamiento, sea cual sea la denominación que éstos reciban, sino de un régimen sancionatorio expreso, como de una institucionalidad que permita un control y ámbito de garantía efectivo del derecho al habeas data.

La anterior afirmación se precisa, por cuanto es necesario entender que este derecho, como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben pender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones.”

Modelo Híbrido

Colombia ha tomado el camino mixto o híbrido¹⁷⁹, al seleccionar de los dos modelos de protección de datos personales los elementos que el legislador considera importantes: mayormente del modelo europeo, una autoridad pública central que vigila, una norma general, cuyos principios son aplicables a las normas especiales, y varios mecanismos de tutela jurídica; del modelo norteamericano ha tomado las regulaciones sectoriales con las normas dictadas en materia de la historia clínica y del dato comercial, crediticio y financiera, por mencionar unos ejemplos.

La Corte Constitucional así lo afirma fundamentado en que las disposiciones generales no contienen regulaciones necesarios para algunos tipos de datos personales que se relacionan con el ejercicio de otras libertad y derechos fundamentales: por ejemplo la historia clínica que se relaciona con el derecho a la salud y a la vida; la información periodística relacionada con el derecho a la libertad de expresión; el dato comercial o financiero, relacionado con el derecho al buen nombre y a la honra. Estas disposiciones especiales deben cumplir con el trámite de una ley estatutaria, cuyos contenidos se deduce que van a”(...) *(i) perseguir una finalidad constitucional, (ii) prever medios idóneos para lograr tal objetivo, y (iii) establecer una regulación que en aras de la finalidad perseguida, no sacrifique de manera irrazonable otros derechos constitucionales, particularmente el derecho al habeas data. Además, de conformidad con los principios que se examinarán más adelante, el cumplimiento de las garantías y la limitación del habeas data dentro de los límites de la proporcionalidad debe ser vigilada y controlada por un órgano independiente, bien sea común o sectorial*” (Sentencia C-748 de 2011 MP Jorge Pretelt Chaljub)

En la ley 1581 de 2012 se regula el modelo de protección de datos personales que se establece en Colombia para desarrollar el artículo 15 de la Constitución y se compone de los siguientes elementos:

¹⁷⁹“En consecuencia, con la introducción de esta reglamentación general y mínima aplicable en mayor o menor medida a todos los datos personales, el legislador ha dado paso a un sistema híbrido de protección en el que confluye una ley de principios generales con otras regulaciones sectoriales, que deben leerse en concordancia con la ley general, pero que introduce reglas específicas que atienden a la complejidad del tratamiento de cada tipo de dato.”

- Sujetos intervinientes en el tratamiento de datos personales (titular del derecho, responsable del tratamiento, encargado del tratamiento)
- Principios rectores del debido tratamiento de datos personales
- Bien jurídico del dato personal (dato personal, bases de datos personales, tipos de datos personales)
- Hechos jurídicos (el tratamiento, la autorización)
- Derechos de los titulares del dato personal
- Obligaciones de los encargados y responsables del tratamiento
- Procedimientos y mecanismos para la protección de datos personales
- Condiciones previas para el tratamiento de datos personales

Sujetos intervinientes

La ley define a tres sujetos intervinientes en todo el proceso de tratamiento de datos personales, sin embargo según el profesor Nelson Remolina (2013:118) quedó fuera un cuarto actor que es la persona que utilice los datos personales, pues queda sin obligaciones legales acerca de la manera como se deben utilizar los datos para que sea legítimo.¹⁸⁰

La amplitud de los intervinientes permite que se incluya cualquier persona sin importar su origen, privado o público, ni su naturaleza jurídica o natural. Para la Corte Constitucional ese término “entidades” permite esa amplitud, así lo manifestó en sentencia C-748 de 2011:

“Así, en atención a los principios de interpretación conforme a la Constitución y de conservación del derecho, la Sala concluye que debe entenderse –sin necesidad de condicionar la exequibilidad del precepto- que la interpretación del inciso que se ajusta a la Carta es aquella según el cual el término *entidades* comprende tanto las personas naturales como jurídicas. De modo que así entendida la condición, la Sala también concluye que es compatible con la Carta, pues cobija las hipótesis necesarias para que el proyecto cumpla su finalidad de brindar protección a los datos personales. “

¹⁸⁰ No se incluyen los operadores y fuentes de la información que menciona la ley 1266 porque se asemejan al encargado y responsable del tratamiento para efectos de la ley 1581 de 2012.

Que cualquier entidad pueda ser responsable o encargado del tratamiento de datos personales, no implica que puedan entremezclarse ambos roles. Con precisión la LEPDP señaló la existencia de esos roles porque con lleva una serie diferente de obligaciones durante el tratamiento de datos personales que permite un grado diferente de sanción¹⁸¹. En efecto, como se vio anteriormente el responsable se encarga de dar las directrices sobre el uso de los datos, a través de la política de tratamiento de datos personales, y recabar el consentimiento del titular del dato; el encargado tiene la obligación de realizar el tratamiento para las finalidades que estableció el responsable, pudiendo ser autónomo en la selección de medios y en las políticas de seguridad de la información.

A pesar de lo anterior la Corte Constitucional en sentencia C-748 de 2011¹⁸² no limita a los intervinientes identificados en la norma como los únicos a los cuales se les puede exigir el cumplimiento de la LEPDP y para mella entran todo aquel que este involucrado de alguna manera en el tratamiento de datos personales. Para la Corte importa verdaderamente la realidad y no las formas o nominaciones de los sujetos intervinientes.

Aun así pueden afirmarse las siguientes definiciones a partir del análisis efectuado en sentenci C-741 de 2011:

El titular del dato personal es la persona natural o jurídica que entrega la información personal concerniente por cualquier medio, físico o electrónico.

Responsable del tratamiento: A partir del análisis de la definición que realiza la Corte Constitucional¹⁸³ puede decirse que es aquella persona jurídica o natural que se encarga, sola

¹⁸¹ En virtud del principio de legalidad es necesario definir los sujetos y las sanciones a aplicar.

¹⁸² Sin embargo, se debe señalar desde ahora, al igual que se indicó en la sentencia C-1011 de 2008, que todos los principios de la administración de datos personales identificados en este proyecto –los cuales serán estudiados en otro acápite- son oponibles a todos los sujetos involucrados en el tratamiento del dato, entendiéndose en la recolección, circulación, uso, almacenamiento, supresión, etc., sin importar la denominación que los sujetos adquieran, es decir, llámense fuente, responsable del tratamiento, operador, encargado del tratamiento o usuario, entre otros. Hechas estas aclaraciones, pasa la Sala a examinar la constitucionalidad de las definiciones.” (Sentencia C-748 de 2011)

¹⁸³“(…) el responsable del tratamiento es definido como la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decide sobre la base de datos y/o el tratamiento de los datos.”

o conjuntamente¹⁸⁴, de recolectar la información y el consentimiento del titular del dato personal según los principios de la LEPDP. Según la Corte Constitucional se diferencia del encargado en que determina¹⁸⁵ la finalidad y el medio para hacer el tratamiento de la base de datos, por estos dos aspectos es que puede elegir al encargado y que recae sobre el el peso de la responsabilidad civil¹⁸⁶. “El Dictamen 1/2010 señala que lo que permite identificar al responsable de otros agentes que participan en el proceso, es que él es el que determina los fines y los medios esenciales del tratamiento de los datos. (...)”¹⁸⁷ (Sentencia C-741 de 2011). Esta diferencia la deduce del documento de trabajo de la WP169 de la Unión Europea (2010:1)

La Corte Constitucional ejemplifica así el concepto:

“Así, por ejemplo, será responsable del dato el hospital que crea la historia clínica de su paciente, la universidad o las instituciones educativas en relación con los datos de sus alumnos, pues estos determinan la finalidad (en razón de su objeto que, puede estar señalado en una ley o por el giro normal de la actividad que se desarrolla) para la recolección de los datos, así como la forma en que los datos serán procesados, almacenados, circulados, etc. “

Encargado del tratamiento: Es la persona natural o jurídica, pública o privada que realiza el tratamiento de datos solo o junto a otros, siguiendo las instrucciones del responsable del

¹⁸⁴ Al respecto es ilustrativo el dictamen 1/2010 del Grupo del Artículo 29 sobre lo que se entiende por “conjunto”, pertinente por inspirarse el legislador de la LEPDP en el modelo europeo: “Desde este punto de vista, existe control conjunto cuando las diferentes partes determinan, respecto de unas operaciones de tratamiento específicas, o bien los fines o bien aquellos elementos esenciales de los medios que caracterizan al responsable del tratamiento” (UE,2010:21) Igualmente cuando ambos están gestionando la inclusión de datos personales cuyo consentimiento se obtuvo del titular.(UE,2010:23). Estos criterios junto a otros prácticos se agrupan en la noción de *reparto del control*, que expresa la idea de que las actividades de un responsable del tratamiento son divididas en fases determinadas para cada interviniente, esto lo hacen de común acuerdo. Una figura similar en el derecho colombiano es la de la coautoría, que cumple los mismos efectos en materia de determinación de la responsabilidad penal.

¹⁸⁵Esto va en consonancia con lo afirmado por el dictamen 1 de 2010 del Grupo del Artículo 29 (UE, 2010:10): “El enfoque de hecho también se ve respaldado por la consideración de que la Directiva establece que el responsable del tratamiento es quien «determin[a]» más que quien «determina legalmente» los fines y los medios.”

¹⁸⁶ Dice el Dictamen 1/2010(UE, 2010:4) “Por último, no es sorprendente que el responsable del tratamiento también deba responder, en principio, del perjuicio resultante de un tratamiento ilícito (artículo 23).”

¹⁸⁷Estos aspectos generalmente están incluidos en la política de tratamiento de la información personal. Los medios técnicos y organizativos pueden dejarse al encargado del tratamiento.

tratamiento, plasmadas mediante un acto jurídico contractual. Se entiende el tratamiento como todos los procedimientos de recolección, almacenamiento, análisis, modificación, eliminación de datos personales así como las medidas técnicas para realizar estas actividades de manera segura. Se requiere que sea independiente totalmente del responsable, no esté vinculado administrativamente a las decisiones que tome, es decir, sea parte de un grupo empresarial (UE, 2010:1 y 6)

Puede ser también responsable si encuadra de manera real con la descripción de responsable del tratamiento, en ese caso le será exigible el cumplimiento de los deberes del mismo.

Para definir quien es encargado la Corte utiliza el criterio de la *delegación con instrucciones*¹⁸⁸ que ejemplifica así:

“(...) el encargado recibe unas instrucciones sobre la forma como los datos serán administrados. Volvamos al ejemplo de la historia clínica, en el que la institución de salud contrata con una compañía el procesamiento de las historias para que con un programa especial que puede determinar el responsable o la empresa contratada, le organice la información contenida en ellas, siguiendo las indicaciones que establece el hospital. En este caso, el encargado del tratamiento de los datos es la persona jurídica que se contrata para el procesamiento de las hojas de vida. “(Sentencia C-748 de 2011)
(...)”

Finalmente, como ejemplifica la Directiva referida –ejemplos que la Sala considera también son aplicables a nuestro caso, el responsable del tratamiento puede surgir: (i) cuando en el cumplimiento de una determinada función, se impone la recolección de datos, por ejemplo, en el caso de la seguridad social; la directiva en comento denomina esta situación *competencia legal explícita*; (ii) cuando en el ámbito propio de la actividad se produce el

¹⁸⁸“De otro lado, el criterio de delegación coincide con el término “por cuenta de” utilizado por el literal e), lo que da a entender una relación de subordinación del encargado al responsable, sin que ello implique que se exima de su responsabilidad frente al titular del dato.” (Sentencia C-748 de 2011)

tratamiento, se trata del caso de los empleadores frente a sus trabajadores, lo que se denomina *competencia jurídica implícita*; y (iii) cuando sin existir las competencias anteriores, se tiene la capacidad de determinación, hecho que se denomina *capacidad de influencia de hecho*.

Principios rectores del debido tratamiento de datos personales

El Congreso de Colombia tomó la decisión de fijar unos principios generales para el tratamiento de datos personales al existir una diversidad de normativas para sectores como la salud, censo, telecomunicaciones finanzas y comercio.

En la medida que establecen los aspectos esenciales, al momento de realizar el tratamiento para no vulnerar los derechos fundamentales, deben ser entendidos en los términos de la teoría del profesor Robert Alexy en “(...) tanto en la jurisprudencia como en el ámbito internacional se han fijado una serie de principios para la administración de datos personales, que como mandatos de optimización, tiendan a facilitar la labor de ponderación entre las prerrogativas constitucionales en tensión.”

Puede afirmarse que los principios rectores establecen cuales son los valores o cualidades importantes que deben incorporarse a cada una de las actividades de tratamiento de la información. En el ordenamiento jurídico constitucional los valores principales protegidos son la libertad y la dignidad humana, como bien lo interpreta la Corte Constitucional, porque permiten considerar al ser humano como sujeto autónomo a quien debe dejársele el ejercicio de su deseos y satisfacciones en la mayor medida posible para lograr su perfeccionamiento.(Ver jurisprudencia sobre la dignidad como valor)

Los principios rectores de la administración de datos personales son el desarrollo del artículo 15 de la Constitución colombiana para prevenir que se afecten los derechos y libertades con el tratamiento de la información

Los principios que reconoce la normativa colombiana¹⁸⁹ son:

Principio de licitud y lealtad: Los tratamientos de datos personales deben darse bajo normas vigentes del país y la buena fe de la persona que entrega sus datos personales. La Corte Constitucional lo describe así:

“El principio encierra el principal objetivo de la regulación estatutaria: someter el tratamiento de datos a lo establecido en las normas, fijar límites frente a los responsables y encargados del tratamiento y garantizar los derechos de los titulares de los mismos. En estos términos, tal y como se explicó anteriormente, a partir del principio de libertad, la jurisprudencia constitucional señaló que el dato debía ser adquirido, tratado y manejado de manera lícita.” Sentencia C-748 de 2011

Principio de transparencia: Es concordante con el artículo 11 y 12 de la ley 1581 de 2012. Establece la necesidad de que las personas conozcan y sean informadas acerca del tratamiento en cualquier momento y de manera sencilla y expedita. Al mismo tiempo debe ofrecer completo conocimiento de los intervinientes en el tratamiento, identificándolos adecuadamente. La Corte Constitucional enuncia los requisitos para cumplir este principio:

“(…) (i) información sobre la identidad del controlador de datos, (ii) el propósito del procesamiento de los datos personales, (iii) a quien se podrán revelar los datos, (iv) cómo la persona afectada puede ejercer cualquier derecho que le otorgue la legislación sobre protección de datos, y (v) toda otra información necesaria para el justo procesamiento de los datos.” Sentencia C-748 de 2011.

Principio de calidad de los datos: La información proporcionada por las personas debe ser verídica, así como también la que esté almacenada en los ficheros computarizados reflejar consonancia con la realidad. Las personas pueden ejercer acciones para que se respete este principio.

¹⁸⁹Son inspirados, en algunas ocasiones casi que tomados textualmente, de varias normas internacionales como la Directiva 95/46/CE, la Resolución 45/95 de la ONU.

Principio del consentimiento informado del titular de los datos: Solo es posible la realización de la recolección, almacenamiento y tratamiento cuando la persona dueña de esos datos lo autorice conscientemente o el responsable del tratamiento consienta su realización contando con el permiso. Ese consentimiento debe ser previo, claro e informado acerca de las condiciones técnicas y legales en que se tratarán. Se obvia cuando son datos personales hechos públicos o interés social prevalente. Su materialización se encuentra explícito en los artículos 9° y 10, también tangencialmente en los artículos: 3-a) (definición de autorización), 6-a)(consentimiento para tratar datos sensibles) y 8-e)(derechos del titular a revocar el consentimiento). Manifiesta el derecho de oponerse.

Adicionalmente el consentimiento debe ser específico, de acuerdo a la finalidad establecida en la relación contractual o la protección del interés jurídico ordenado. Fuera de esto se está violando abiertamente el principio cuando se aplique a otros fines, salvo que se informe y la persona consienta en ello, sea capaz de dar este y se permita legalmente.

Principio de la seguridad de los datos: Las personas deben informársele cuales son las medidas técnicas que dispondrá para la conservación y acceso de la información, que medidas jurídicas fijará para la protección. La Corte Constitucional hace una precisión importante respecto a las consecuencias de este principio:

“Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

De este principio se deriva entonces la responsabilidad que recae en el administrador del dato. El afianzamiento del principio de responsabilidad ha sido una de las preocupaciones actuales de la comunidad internacional, en razón del efecto “diluvio de datos. (...)” Sentencia C-748 de 2011.

Principio de confidencialidad de los datos: Desarrollado en el artículo 13 de la ley 1581 de 2012. Implica la obligación de limitar el acceso a las personas que estén autorizadas por el responsable o encargado, poniendo en estos el deber de seleccionar cuidadosamente las más indicadas, de tal forma que no se termine usando para otros fines o entregando a personas irresponsables de sus deberes.

Principio de libertad: Las personas en su dignidad humana, tienen la capacidad de elegir si desean que sea tratados sus datos o no desean que se continúe con el tratamiento. Salvo que así lo ordene la ley. Por esta razón para que se hable del ejercicio de este principio deben darse con total conciencia de los fines que se está dando a sus datos personales¹⁹⁰. La Corte tiene un planteamiento más detallado:

“Este principio, 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.” (Sentencia C-748 de 2011)

Así mismo definió la necesidad del principio de transparencia y de una claridad suficientes para que el titular del dato no de un consentimiento engañado, para que después su libertad sea determinada por otros. En sentencia C-1011 de 2008 lo ratifica:

“Para la Constitución, la libertad del sujeto concernido significa que la administración de datos personales no pueda realizarse a sus espaldas, sino que debe tratarse de un proceso transparente, en que en todo momento y lugar pueda conocer en dónde está su información personal, para qué propósitos ha sido recolectada y qué mecanismos tiene a su disposición para su actualización y rectificación. La eliminación de la autorización previa, expresa y suficiente para la incorporación del dato en los archivos y bancos de datos administrados por los operadores permite, en últimas, la ejecución de

¹⁹⁰ En relación al carácter expreso del consentimiento para conservar la libertad la Corte constitucional expresó que] (...) la jurisprudencia constitucional ha exigido tal condición y ha dicho que el consentimiento debe ser expreso y concreto a la finalidad específica de la base de datos. (...) se traducía también en la prohibición de otorgarse autorizaciones abiertas y no específicas.” (C-748 de 2011)

actos ocultos de acopio, tratamiento y divulgación de información, operaciones del todo incompatibles con los derechos y garantías propios del hábeas data. (Resaltado fuera del texto) (Sentencia C-1011 de 2008)

De todo lo anterior, puede entonces deducirse: (i) los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo, expreso e informado del titular. Es decir, 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 y (iii) el principio de libertad no sólo implica el consentimiento previo a la recolección del dato, sino que dentro de éste se entiende incluida la posibilidad de retirar el consentimiento y de limitar el plazo de su validez.

Principio de finalidad: Todo tratamiento de datos personales debe iniciarse con un propósito en mente por parte del responsable, que debe ser comunicada de forma clara, temporal y precisa. Es necesario que sea así para evitar sorpresas o molestias respecto al titular, quien lo autoriza para un fin y termina enterándose de que fue utilizado en otro. Con este fin viene también la proporción del dato, es decir, pedir datos adecuados conforme al fin seleccionado y expresado al titular. La Corte Constitucional colombiana lo expresó así en sentencia C-748 de 2011:

“Así mismo, los datos personales deben ser procesados sólo en la forma que la persona afectada puede razonablemente prever. Si, con el tiempo, el uso de los datos personales cambia a formas que la persona razonablemente no espera, debe obtenerse el consentimiento previo del titular.

Por otro lado, de acuerdo la jurisprudencia constitucional y los estándares internacionales relacionados previamente, se observa que el principio de finalidad implica también: (i) un ámbito temporal, es decir que el periodo de conservación de los datos personales no exceda del necesario para alcanzar la necesidad con que se han registrado y (ii) un ámbito material, que exige que los datos recaudados sean los estrictamente necesarios para las finalidades perseguidas.”

Principio de acceso y circulación restringida: Este principio es una consecuencia del principio de finalidad y del principio de confidencialidad en los datos personales. En efecto si se usan para los fines establecidos y por las personas autorizadas, el responsable debe garantizar que ellos cumplan con la no divulgación y uso para otros objetivos diferentes, con ello se restringe y se limita automáticamente el acceso a datos que por principio no son públicos o accesibles fácilmente.

Principios derivados directamente de la Constitución

La Corte Constitucional señala tres principios: el de prohibición de discriminación, el de interpretación integral de los derechos constitucionales y el principio de indemnizar por los perjuicios causados. Estos principios provienen directamente de la constitución, en virtud de considerar la dignidad del ser humano y la eficacia de sus derechos fundamentales.

Principio de necesidad

“En relación con el principio de necesidad, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, 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. Sobre el particular, la Sentencia T-307 de 1999, afirmó: *“la información solicitada por el banco de datos, 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”.”(Sentencia C-748 de 2011)

Principio de utilidad

En virtud de éste, la ausencia de la misma se traduce en un abuso del derecho. En este sentido, en la sentencia T-119 de 1995, la Corte consideró que la sola autorización de funcionamiento de las entidades administradoras de datos, no constituía garantía de la legitimidad de sus conductas.”. En consecuencia, tanto el acopio, el procesamiento y la divulgación de los datos personales, *“debe cumplir una función determinada, como expresión del ejercicio legítimo del derecho a la administración de los mismos; por ello, está prohibida la divulgación de datos que, al carecer de función, no obedezca a una utilidad clara o determinable.”* (Sentencia C-748 de 2011)

Principio de integridad en el manejo de los datos

“En la sentencia SU-082 de 1995, esta Corporación fijó el principio de integridad en el manejo de los datos. Bajo su amparo, se prohibió que el manejo de los datos fuese incompleto, en razón a que esta situación puede distorsionar la veracidad de la información. (...) En consecuencia, en virtud de aquél principio “la información que se registre o se divulgue a partir del suministro de datos personales debe ser completa, de tal forma que se encuentra prohibido el registro y divulgación de datos parciales, incompletos o fraccionados. Con todo, salvo casos excepcionales, la integridad no significa que una única base de datos pueda compilar datos que, sin valerse de otras bases de datos, permitan realizar un perfil completo de las personas.” (Sentencia C-748 de 2011)

Principio de incorporación: En la sentencia T-307 de 1999 la Corte determinó el alcance del principio de la incorporación. Allí, se estudió el caso de una actora que después de intentar infructuosamente durante varios años su inclusión al régimen subsidiado de salud mediante el sistema SISBEN, nunca pudo disfrutar de los beneficios en razón del mal manejo de la

información. Por ello, a partir de la existencia del llamado *habeas data* aditivo, se dijo cuando de la inclusión de datos personales en determinadas bases, deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos, si el titular reúne los requisitos que el orden jurídico exija para tales efectos, de tal forma que queda prohibido negar la incorporación injustificada a la base de datos.

Principio de caducidad: Una vez que se cumpla la finalidad perseguida con el tratamiento no deben conservarse por más tiempo, deben cancelarse y eliminarse. Si no se realiza, la persona tiene el derecho de exigirlo. En principio de la integridad y calidad del dato personal surge este principio negativo, en cuanto a que establece límites al tratamiento sucesivo y eterno de los datos del titular.

Principio de individualidad: establece que no está permitido un cruce indiscriminado de bancos de datos para conformar perfiles virtuales de las personas. Pues dice la Corte Constitucional en sentencia C-748 de 2011 que establecer “correlaciones entre datos que aisladamente son las más de las veces inofensivos pero que reunidos pueden descubrir aspectos cuya revelación atenta contra la libertad e intimidad del ciudadano.”

Principios derivados del núcleo temático del proyecto de ley estatutaria

Estos principios son mencionados por la Corte Constitucional porque se encuentran de manera transversal en la LEPDP, pese a que no se encuentran enunciados, así a continuación los describe como:

- (i) Principio de la proporcionalidad del establecimiento de excepciones: La Ley consagra materias exceptuadas, más no excluidas, del régimen general de la administración de datos, tal y como se explicó en el análisis del ámbito de aplicación de la norma. Sin embargo, tal tratamiento especial debe estar justificado en términos de proporcionalidad y responder a los estándares internacionales de protección,

- (ii) Principio de autoridad independiente: la adopción de una normatividad sólo es efectiva si se garantiza que dentro de la estructura del Estado exista un órgano encargado de garantizar el respeto de los principios anteriormente desarrollados. Esta autoridad debe garantizar imparcialidad e independencia y
- (iii) Principio de exigencia de estándares de protección equivalentes para la transferencia internacional de datos: Tal y como se deduce del artículos 26 del Proyecto de Ley Estatutaria, existe una prohibición de transferencia internacional a cualquier tipo de países que no proporcionen niveles adecuados de protección de datos.

El Dato personal: Bien jurídico protegido por el Habeas Data (dato personal, bases de datos personales, tipos de datos personales)

Definición: “Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”

Se enuncia lo que ha dicho la Corte Constitucional respecto a las características de los datos personales: “(...) 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.”(Sentencia C-748 de 2011)

Vigencia del dato personal:

En cabeza del responsable del tratamiento de datos personales, pues estos son por naturaleza mutables, a fin de evitar que se circulen perfiles virtuales falsos o inmutables de una persona, eliminando su oportunidad de mejorarlo o actualizarlo, situación que vulnera el derecho al buen nombre y a la honra. Aquí hay situaciones polémicas como el derecho al olvido, la

prescripción de una obligación como cancelación de un dato, que es cancelación y que es actualización, como se justifica la existencia de archivos históricos.

Bases de Datos personales

El artículo 3 de la ley 1581 de 2012 define las bases de datos como “*conjunto organizado de datos personales que sea objeto de tratamiento*”, en esta definición se aprecian dos elementos importantes de la definición: i) conjunto organizado de datos personales ii) ser objeto de tratamiento.

i) La definición de base de datos como “*conjunto organizado de datos personales (...)*” permite una amplitud en su aplicación¹⁹¹ e incluye los archivos de documentos¹⁹², puesto que representan una forma rudimentaria de tratamiento de la información como es la organización de soportes acumulados en el ejercicio de las actividades de una empresa o entidad pública.¹⁹³ El criterio de ser un “conjunto organizado” excluye aquel conjunto de información que se tiene almacenado en forma desordenada y sin un criterio claro de aprovechamiento, porque se presume que cuando se realizan labores de organización de la información, con cualquier clase de criterio, se busca obtener alguna conclusión que no es tan sencilla de extraer con la información puramente recolectada y almacenada. Adicionalmente en vista de que no se hace referencia al proceso de organizado o tratamiento de la información como elemento integrante de la definición legal, debemos remitirnos al artículo 2° de la ley 1581 donde al final del inciso primero se afirma que éstas deben ser “*(...) susceptibles de tratamiento por entidades de naturaleza pública o privada.*”

¹⁹¹De hecho la misma Corte Constitucional hace más flexible el uso del término al ser aplicable a cualquier información personal que reciba alguna forma de tratamiento, siendo esencial esto último para que se llame así. (Ver consideración 2.4.3.2 de la Sentencia C-748 de 2011 MP Jorge Pretelt Chaljub)

¹⁹² “De acuerdo con estas definiciones, los archivos –para efectos exclusivamente del proyecto-, en tanto son (i) depósitos ordenados de datos, incluidos datos personales, y (ii) suponen, como mínimo, que los datos han sido recolectados, almacenados y, eventualmente, usados –modalidades de tratamiento, son una especie de base de datos que contiene datos personales susceptibles de ser tratados y, en consecuencia, serán cobijados por la ley una vez entre en vigencia.” (Sentencia C-748 de 2011 MP Jorge Pretelt Chaljub MP Jorge Pretelt Chaljub)

¹⁹³Para una definición más amplia y detallada es adecuado revisar el artículo 3 de la ley 594 de 2000, “por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”

La definición es tan amplia para garantizar la extensión de la protección del derecho y no existan fugas que vulneren la dignidad humana u otros derechos importantes, esto se apoya en lo que afirma el profesor Nelson Remolina (2013:123) al decir que “(...) la finalidad de la ley es exigir unos mínimos en el uso de los datos para no lesionar derechos de las personas, con independencia de si los datos están contenidos en sistemas de información elementales, complejos o avanzados”.

ii) El ser objeto de tratamiento significa que sobre ese conjunto de datos personales se ejerza algunas de las operaciones reconocidas internacionalmente como tratamiento de datos personales: recolección, modificación, uso (en el sentido más amplio y recuérdese que limitado a la finalidad), la circulación o la supresión.

Las bases de datos personales reguladas por la LEDPD son definidas, para efectos de este trabajo luego del análisis integrador de la misma, como un conjunto organizado de datos personales con el objeto de recibir alguna clase de tratamiento (uso, recolección, análisis, transmisión) por parte de cualquier persona natural o jurídica ubicada en territorio colombiano.

Bases de datos excluidas

La razón de que existan excepciones en las bases de datos se debe ellas generan una colisión entre el derecho al habeas data y otros derechos fundamentales como la intimidad (literal a), la salud, el principio de la seguridad nacional, para establecer regímenes de excepción en las bases de datos, los cuales deben regularse por leyes específicas que se expidan posteriormente.¹⁹⁴. El artículo 2° de la LEDP estableció un conjunto de bases de datos a los

¹⁹⁴Así lo afirma la Corte Constitucional en Sentencia C-748 de 2011 MP Jorge Pretelt Chaljub: “En otras palabras, las hipótesis enunciadas en el inciso tercero son casos exceptuados –no excluidos- de la aplicación de las disposiciones de la ley, en virtud del tipo de intereses involucrados en cada uno y que ameritan una regulación especial y complementaria, salvo respecto de las disposiciones que tienen que ver con los principios”

cuales se les aplica solo los principios de tratamiento de datos personales y se excluye todas los demás artículos de ella, a continuación se mencionan cuales son:

- El literal a) establece la excepción de las bases de datos que se mantengan para fines propios del ámbito privado o doméstico de la persona natural, esto excluye a las personas jurídicas quienes no gozan de tener una esfera íntima imperturbable, pues dice la Corte Constitucional que “(...) *los ámbitos personal y doméstico son las esferas con las que tradicionalmente ha estado ligado el derecho a la intimidad, el cual, en tanto se relaciona con la posibilidad de autodeterminación como un elemento de la dignidad humana, no puede predicarse de las personas jurídicas*”. Esta excepción se pierde cuando la persona suministre los datos o cambie los fines de uso¹⁹⁵, por ejemplo la base de datos de clientes de la persona natural que es comerciante independiente o vendedor, que trabaja para una persona jurídica, que guarda en su teléfono personal los números de contacto de sus clientes (Remolina, 2013:129)
- El literal b) exceptúa las bases de datos que tienen la finalidad de proteger la seguridad y defensa nacional así como el fin de prevenir, detectar o monitorear el lavado de activos y el financiamiento al terrorismo. La exclusión es clara, el Estado colombiano para resguardar el orden constitucional y reprimir el crimen organizado debe realizar actividades de recolección y análisis de datos, entre esos algunos personales, mediante el uso de la tecnología más moderna, frente a lo cual cede parcialmente el derecho al habeas data de cada persona que tenga los datos. (Ver considerando 2.4.5.4 de la sentencia C-748 de 2011 MP Jorge Pretelt Chaljub)
- El literal c) se refiere a bases de datos generadas en actividades de inteligencia y contrainteligencia, que realiza el estado para garantizar la seguridad de los ciudadanos y el Estado, por lo cual dicha información debe permanecer en reserva, por lo menos hasta el límite de realización de la actividad cuando se tenga conocimiento de la posible comisión o tentativa de un delito, y utilizarse para fines preventivos.

¹⁹⁵“Así, en tanto los datos mantenidos en estas esferas (i) no están destinados a la circulación ni a la divulgación, y (ii) su tratamiento tampoco puede dar lugar a consecuencias adversas para el titular, tiene sentido que su tratamiento esté exceptuado de algunas disposiciones del proyecto.” (Sentencia C-748 de 2011 MP Jorge Pretelt Chaljub MP Jorge Pretelt Chaljub)

- El literal d) se refiere a las bases de datos que generan los periodistas para sus actividades profesionales o los medios de comunicación, con el fin de evitar limitaciones a la libertad de expresión y de prensa, inadmisibles en el derecho internacional de los derechos humanos y en la Constitución. Se excluyen las bases de datos en su poder que se usen para otros fines.
- Los literales e) y f) se refieren a tipos de datos personales que son objeto de regulaciones jurídicas especializadas. Así ocurre con la ley 1266 de 2009, sobre el dato comercial, crediticio y financiero y la ley 79 de 1993 sobre datos estadísticos y censales.

Hechos jurídicos: el tratamiento de la información a través de sistemas de información y la autorización del titular del dato personal

Los hechos jurídicos generadores del derecho de protección del dato personal consisten en i) el tratamiento de información personal a través de sistemas de información mecánico o electrónico y ii) la autorización del titular del dato personal.

“El tratamiento es definido como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (...)”

En ese orden, cuando el proyecto se refiere al tratamiento, hace alusión a cualquier operación que se pretenda hacer con el dato personal, con o sin ayuda de la informática, pues a diferencia de algunas legislaciones, la definición que aquí se analiza no se circunscribe únicamente a procedimientos automatizados. Es por ello que los principios, derechos, deberes y sanciones que contempla la normativa en revisión incluyen, entre otros, la recolección, la conservación, la utilización y otras formas de procesamiento de datos con o sin ayuda de la informática.” (Sentencia C-748 de 2011)

El tratamiento de la información se realiza o bien a través de sistemas de información o de métodos mecánicos. Los sistemas de información tienen las siguientes características

(Remolina 2010^a:492): “i)se nutren de datos personales.(ii) Ofrecen innumerables posibilidades para recolectar, almacenar y circular esa información en poco tiempo y de manera imperceptible para las personas a las que se refieren los datos.(iii) No son absolutamente seguros.(iv) Evolucionan rápidamente.(v) Traspasan las fronteras físicas, lo cual facilita el flujo internacional de la información en comento.”

Debido a las múltiples ventajas que ofrecen los sistemas de información y al impacto que pueden generar sobre las personas, se requiere que haya una autorización de cada titular del dato personal. La autorización consiste en la respuesta afirmativa y explícita del titular del dato a la solicitud de tratamiento de información del dato por parte del responsable, siendo requisito previo que se le informe las condiciones de tratamiento de la información, el marco contractual bajo el cual se da el mismo y la finalidad respectiva del tratamiento. “En consecuencia, basta por ahora señalar 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”(…)”(Sentencia C-748 de 2011)

Ambos aspectos son tratados como actos jurídicos porque son una exigencia normativa, cuya omisión genera consecuencias jurídicas a dos niveles: una posible sanción de la Superintendencia de Industria y Comercio y un indicio acerca de la vulneración al tratamiento debido de datos personales; según el derecho que busque proteger el titular del dato podrá seleccionar algunos de los mecanismos más adecuados para la tutela efectiva.

Derechos protegidos por los mecanismos

"El peligro para la privacidad del individuo no radica en que
Se acumule información sobre él, sino, más bien,
En que pierda la capacidad de disposición sobre ella
Y respecto a quién y con qué objeto se transmiten"

Ernesto Benda,
Dignidad humana y derechos de la Personalidad

La autonomía del derecho a la protección de datos personales no le desliga de su origen que es el derecho de intimidad y de los otros derechos fundamentales que tienen relación con el individuo y su proyección social. Todos estos derechos beben de la misma fuente que le permite reafirmarle como ser autónomo: la dignidad de la persona como ser humano.

El derecho a la protección de datos personales, dado su carácter instrumental y centrado en información que tiene unas consecuencias en la valoración de las personas y su consideración por los semejantes hace que funja de manto protector sobre los demás derechos. Esta afirmación nos lleva a justificar que para las herramientas jurídicas que garantizan el habeas data, también de manera indirecta están garantizando los derechos conexos que a continuación se van a exponer.

Derechos Conexos

a) Derecho a la intimidad

Intimidad proviene del vocablo latino *intimus*, que “(...) evoca la idea de lo más interno o recóndito” (Pérez Luño, 2006:130). Se entiende como aquello inaccesible a simple vista, que está secreto. Quienes así la conciben son los mencionados Samuel Warren y Louis Brandeis con el agregado de que nadie puede intentar entrar a ese espacio si no se lo permitimos antes. “La soledad es la forma más perfecta de la vida privada”, dice el profesor García Morente (Cit. en Pérez Luño, 2006:130).

La Corte Constitucional colombiana en sentencia T-414 de 1992 da una definición inicial acerca del derecho a la intimidad como “protección de la vida privada” y se refiere en un “sentido amplio como estricto.”; se habla de intimidad en sentido amplio cuando se referencia la protección de la vida familiar y personal, en sentido estricto “(...) la protección de las personas contra atentados que afectan particularmente el secreto o la libertad de la vida privada”, así el énfasis de cada uno es preventivo y reactivo, respectivamente.

La Corte Constitucional, en un considerando de la sentencia mencionada arriba, detalla un poco más la intimidad así: “La misma doctrina destaca también que la intimidad se proyecta en dos dimensiones a saber: como secreto de la vida privada¹⁹⁶ y como libertad. Concebida como secreto, atentan contra ella todas aquellas divulgaciones ilegítimas de hechos propios de la vida privada o familiar o las investigaciones también ilegítimas de acontecimientos propios de dicha vida. Concebida como libertad individual, trasciende y se realiza en el derecho de toda persona de tomar por sí sola decisiones que concierne a la esfera de su vida privada. ” (Sentencia T-414 de 1992, MP Ciro Angarita Barón)

Puede apreciarse como se incorpora a la faceta individualista del derecho que inicialmente se planteó como “right to be alone” en el sentido general antes mencionado y como la toma de interés por el control de lo que se hace con nuestra vida, a través de la información que conocen de nosotros, la vuelve más activa, en el sentido estricto, para perseguir los autores de las vulneraciones (público o privados) y garantizar la efectiva libertad, el derecho a la personalidad y la dignidad humana. “En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada. Su finalidad es la de asegurar la protección de intereses morales; su titular no puede renunciar total o definitivamente a la intimidad pues dicho acto estaría viciado de nulidad absoluta” (Sentencia T-486 de 1992)

Recordando lo anterior se afirma que se ha vulnerado la intimidad ante el indebido tratamiento de datos personales cuando se recolectan datos que exceden del ámbito

¹⁹⁶La sentencia T-552 de 1997 describe como un “(...) un ámbito exclusivo que incumbe solamente al individuo, que es resguardo de sus posesiones privadas, de sus propios gustos y de aquellas conductas o actitudes personalísimas que no está dispuesto a exhibir, y en el que no caben legítimamente las intromisiones externas.”

estrictamente informado al titular para que autorizara, cuando se recaban datos que pertenecen al ámbito exclusivo de la familia o cuando se traiciona la confianza depositada en los responsables del tratamiento.

b) Derecho al olvido

Este derecho se reconoce para prevenir que la larga vigencia del dato personal negativo de una persona afecte su buen nombre. Son tres los principios del tratamiento del dato personal que apoyan este derecho: el principio de veracidad, caducidad e integridad de la administración de datos personales.

El principio de caducidad existe para evitar que el registro o dato negativo permanezca mucho más allá del tiempo razonable para que otras personas puedan informarse acerca de una situación específica del titular del dato, no solo importa el criterio de veracidad también el hecho de que está prohibido el uso de bases de datos históricas negativas. Podría pensarse que se afecta el derecho al buen nombre, sin embargo este solo puede reclamarse cuando allá sido por un error del encargado del registro del dato y no por la conducta de la persona que dio origen al dato. Otro caso específico es cuando ocurre la prescripción de la obligación que lleva a la automática caducidad del dato en el registro sin que se requiera orden judicial (Sentencia T-022 DE 1993 y sentencia T-486 de 1992) debido a la falta de actualidad del dato.

Al respecto la Corte Constitucional en sentencia T-414 de 1992 confirma los principios mencionados que son fundamentos del derecho al olvido:

“Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de "personas virtuales" que afecten negativamente a sus titulares, vale decir, a las personas reales.

De otra parte, es bien sabido que las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia después de algún tiempo tales personas son titulares de un verdadero derecho al olvido.”

La Corte define el cumplimiento de unos presupuestos para modificar el dato de la situación de la persona a la actual y eliminar el anterior (Sentencia T-157 y T-164 de 1994): i) manifieste que ocurrió la prescripción de la obligación y ii) se realice una solicitud de tutela transitoria del derecho al habeas data mientras se profiere la sentencia por parte de la jurisdicción ordinaria competente.

El principio de veracidad como derecho se manifiesta mayormente en el dato personal negativo, que se conserva en la base de datos y no representa la situación actual de una persona, esta desactualización estaría afectando el derecho al olvido de la persona y si se divulgue el derecho al buen nombre de la persona, quien ya “rehabilitó” su reputación social o comercial al cumplir la obligación.

El principio de integridad nos explica que el tratamiento de datos personales debe realizarse sobre datos que sean completos y no permitan una confusión acerca de la situación actual de una persona, este principio surge para evitar que se tomen decisiones perjudiciales por las personas que acceden a la información desactualizada almacenada en las bases de datos.

c) Derecho al buen nombre¹⁹⁷

La honra y el honor cuando la información desestima el valor social de la persona y el valor propio que tiene de ella¹⁹⁸. Hay un derecho que está íntimamente vinculado con estos

¹⁹⁷Algunas sentencias que desarrollan el buen nombre en vinculación con el habeas data: T-814 DE 2003, SU-089 de 1995, SU-056 de 1995.

¹⁹⁸ “El buen nombre alude al concepto que del individuo tienen los demás miembros de la sociedad en relación con su comportamiento, honestidad, decoro, calidades, condiciones humanas y profesionales, antecedentes y ejecutorias. Representa uno de los más valiosos elementos del patrimonio moral y social de la persona y constituye factor indispensable

que es el buen nombre e imagen, que se vulnera cuando se genera una imagen que resta reconocimiento o nos da una apariencia errada a otros; respecto al habeas data hace parte del Habeas Data rectificatorio o cancelatorio.

Claro que para tener buen nombre es necesario que la persona se comporte con decoro y acorte a la costumbre social esperada de él en sus relaciones sociales¹⁹⁹, lo cual se desarrolla mercedamente través de “la conducta irreprochable de quien aspira a ser su titular y el reconocimiento social del mismo. En otros términos, el buen nombre se adquiere gracias al adecuado comportamiento del individuo, debidamente apreciado en sus manifestaciones externas por la colectividad.” (Sentencia T-229 de 1994. Magistrado Ponente Dr. José Gregorio Hernández). Sin embargo esto no es justificación para acometer burlas o tratos denigrantes contra la persona que no tiene buena reputación social.

En una curiosa consideración (Octava de la sentencia SU-082 de 1995) la Corte afirma, a favor de la persona que cumple sus obligaciones a tiempo, que surge el derecho de que esto sea anotado en la base de datos para acrecentar su buen nombre tanto así como el que es incumplido y se le reporta el dato negativo pero cierto acerca de esa mora. Es algo totalmente razonable que así sea, pues de lo que se trata es de que se den los datos lo más completos posibles y no se omita parcialmente la verdad.

Si queremos de verdad aprovechar los beneficios de las nuevas tecnologías en el tratamiento de la información para las personas debe darse un trato igualitario de lo positivo como de lo negativo, siempre que reflejen la realidad de los hechos; se estaría dando cumplimiento a dos principios fundamentales en el tratamiento de datos personales: veracidad y calidad.

de la dignidad que a cada uno debe ser reconocida.” Sentencia T-229 de 1994. Magistrado Ponente Dr. José Gregorio Hernández.

¹⁹⁹ Lo anterior implica que no está en posición de reclamar respeto y consideración a su buen nombre quien ha incurrido en actos u omisiones que de suyo generan el deterioro del concepto general en que se tiene al interesado. Así, el que incumple sus obligaciones y persiste en el incumplimiento se encarga él mismo de ocasionar la pérdida de la aceptación de la que gozaba en sociedad y no puede, por tanto, aspirar a que se lo reconozca públicamente como persona digna de crédito. Eso mismo acontece en los diversos campos de la vida social, en los cuales la conducta que una persona observa, cuando es incorrecta, incide por sí sola, sin necesidad de factores adicionales y de una manera directa, en el desprestigio de aquella” Sentencia T-229 de 1994. Magistrado Ponente Dr. José Gregorio Hernández

También existe una afectación al buen nombre cuando se usa el patronímico para denominar a cosas que carecen de fama o para hacer denotar burla y esta situación siga a la persona hasta su ámbito privado. En la misma vulneración se incurre cuando existan imágenes²⁰⁰ de la persona almacenadas en la base de datos y sean utilizadas para fines distintos de los consentidos. Aunque en principio, en opinión de este autor, debería primar la dignidad humana por encima del consentimiento para que sea objeto de burlas con el uso de la imagen.

En cuanto a la conexidad que puede presentarse con el derecho al debido tratamiento de datos personales, está ocurre cuando datos personales que tenga el responsable sean filtrados a terceros, y estos contengan alguna descripción física por la cual pueda ser apodado o tratado peyorativamente. Por ejemplo una persona que tiene en una base de datos de una EPS su historia clínica donde se registra alguna operación, dicho dato sea filtrado y comiencen las burlas fundamentadas en el o los apodos.

El derecho al buen nombre se relaciona con el tratamiento de datos personales en cuanto a que con la recolección de datos personales públicos o semi-privados pueden formarse un concepto o juicio²⁰¹ sobre las personas, lo que afecta la estimación social que se tiene de ellas si no se trata debidamente para el caso de datos ciertos pero negativos²⁰². Un ejemplo de ello reiterado con frecuencia es en cuanto al manejo del crédito donde “(...) es evidente que la fama de buen o mal pagador se origina en la forma en que usualmente la persona atiende sus

²⁰⁰Zavala(1982:95) define imagen como “(...) la proyección o representación gráfica de la figura humana mediante un procedimiento mecánico o técnico”

²⁰¹“La persona es juzgada por la sociedad que la rodea, la cual evalúa su comportamiento y sus actuaciones de acuerdo con unos patrones de admisión de conductas en el medio social y al calificar aquellos reconoce su proceder honesto y correcto. Por lo tanto, no es posible reclamar la protección al buen nombre cuando el comportamiento de la persona no le permite a los asociados considerarla como digna o acreedora de un buen concepto o estimación.” (resaltado fuera de texto) SU-056 de 1995, M.P. Antonio Barrera Carbonell

²⁰²“De otra parte, es claro que el buen nombre es un concepto diferente por completo a la intimidad personal y familiar: ésta es secreta para los demás, en tanto que aquél es público por naturaleza, y lo que es público por naturaleza no puede tornarse en íntimo, porque sería inadecuado.” SU-02 de 1995.

“Eso mismo acontece en los diversos campos de la vida social, en los cuales la conducta que una persona observa, cuando es incorrecta, incide por sí sola, sin necesidad de factores adicionales y de una manera directa, en el desprestigio de aquella”. Sentencia T-094 de 1995.

obligaciones. “(Sentencia SU-082 de 1995, SU-056 de 1995), frente a lo cual quien incumple, en principio será sujeto de sanción social de desconfianza en los negocios, pero esto no puede durar por mucho tiempo. Transcribimos algunos apartes de la sentencia T-094 de 1995, que refiere al derecho fundamental al buen nombre en relación con el habeas data:

“En cuanto a los derechos a la honra y al buen nombre, resultan afectados cuando el banco de datos recoge, maneja o difunde informaciones falsas o cuando, en el caso de las verdaderas, lo sigue haciendo no obstante haber caducado el dato, según los criterios de razonabilidad señalados por la doctrina constitucional.

Es claro que si la información respectiva es falsa o errónea, no solamente se afectan los derechos a la honra y al buen nombre de la persona concernida, sino que, precisamente por el efecto multiplicador que tiene el informe negativo en las instituciones receptoras de la información incorporada al banco de datos o archivo, resulta notoriamente perjudicada en su actividad económica y en su situación patrimonial. No se pierda de vista que un cierre del crédito puede provocar una cadena de incumplimientos forzados, la incapacidad de contraer nuevas obligaciones, la cesación de pagos y la quiebra.

Ahora bien, la jurisprudencia constitucional también ha sido afirmativa al precisar que los derechos a la honra y al buen nombre se tienen únicamente sobre la base del buen comportamiento. El prestigio se aquilata y se fortalece a partir de la bondad de las propias conductas, al paso que sufre deterioro por las fallas en que la persona incurra y por las equivocaciones que cometa.”

d) Derecho a la información

Dentro de la línea jurisprudencial de la Corte Constitucional está ha decantado con prevalencia la protección del derecho a la intimidad y el derecho al habeas data como prioritario frente al derecho a la información. Solamente en unas excepciones ha procedido el

acceso a la información veraz y completa bajo ciertos criterios que se destacan en la sentencia SU-089 de 1995. Estos casos en que prevalece son:

- Que sea información veraz, no importa que sea negativa, en cuanto que no haga un juicio de valor denigrante de la persona.²⁰³
- Que la información sea socialmente relevante con la responsabilidad de usar los medios adecuados de transmisión.²⁰⁴
- Cuando se trata de una actividad de interés público como el crédito, donde las entidades financieras por su seguridad requieren de tener la información más completa sobre las obligaciones contraídas en el pasado por los solicitantes de crédito.²⁰⁵
- Se utilicen medios de difusión adecuados para poder ejercer el cobro de lo adeudado en el caso de los servicios públicos.
- Se haya obtenido el consentimiento para la divulgación y tratamiento de datos personales y este no afecte otros derechos fundamentales.
- Sea necesario cuando se requiere la rectificación de una información que afecte potencialmente al titular del dato y el responsable lo sepa.

e) Derecho al Honor

Este derecho protege el concepto que tenemos de nosotros mismos, es la autoestima y el autorespeto que nos dispensamos. Puede verse afectado por el indebido tratamiento de datos

²⁰³ "(...) la Corte ha avalado la posibilidad de que ciertas entidades privadas, como los bancos, transmitan información de sus clientes a las centrales de riesgo, siempre y cuando la información que transmitan sea veraz, completa y precisa, que para ese caso significa que esté actualizada." (Sentencia T-814 de 2003)

²⁰⁴ "La importancia que socialmente se le otorga a algunos de tales aspectos, implica un mayor compromiso del buen nombre y de la honra de las personas, y por lo tanto, un mayor rigor en el manejo de la información. A manera de ejemplo, puede afirmarse que al transmitir información respecto de la responsabilidad penal de una persona, el emisor debe tener mayor cuidado que cuando se refiere a otros aspectos de la persona. De tal manera, la responsabilidad por la transmisión de la información será mayor o menor, dependiendo de su naturaleza."(Sentencia T-814 de 2003)

²⁰⁵ "En relación con el derecho a la información y la legitimidad de la conducta de las entidades que solicitan información de sus eventuales clientes, a las centrales de información que para el efecto se han creado, así como la facultad de reportar a quienes incumplan las obligaciones con ellos contraídas, tiene como base fundamental y punto de equilibrio, la autorización que el interesado les otorgue para disponer de esa información, pues al fin y al cabo, los datos que se van a suministrar conciernen a él, y por tanto, le asiste el derecho, no sólo a autorizar su circulación, sino a rectificarlos o actualizarlos, cuando a ello hubiere lugar. Autorización que debe ser expresa y voluntaria por parte del interesado, para que sea realmente eficaz, pues de lo contrario no podría hablarse de que el titular de la información hizo uso efectivo de su derecho."(Sentencia T-814 de 2003)

personales en la medida que la proyección de los datos impacte en el valor propio o consideración de la persona, haciéndole padecer trastornos psicológicos como depresión, miedo a las personas.

Dice la Corte Constitucional en sentencia T-442 de 1992 al respecto:

“El contenido esencial de un derecho es aquella parte que le es absolutamente necesaria para que los intereses jurídicamente protegidos y que le dan vida resulten real y efectivamente tutelados.

En el derecho a la honra, el núcleo esencial es el derecho que tiene toda persona a ser respetada ante sí mismo y ante los demás, independientemente de toda limitación normativa.”

f) Derecho a la imagen

Es un derecho subjetivo que le permite a las personas controlar la manera como se captura, usa y configura la imagen de su fisonomía o cuerpo o de alguna parte de este. Dice al respecto Valencia Zea (2006:458) sobre la imagen que “(...) una lesión al derecho de imagen lesiona más directamente la personalidad humana, motivo por el cual el citado derecho actúa en forma independiente del derecho sobre el cuerpo”

Es una consideración de respeto hacia su dignidad humana el que no se instrumentalice la imagen del ser humano sin su permiso, podría esto considerarse una intromisión a la intimidad cuando se hace arbitrariamente, una vulneración al honor cuando hace que desmerezca valor frente a sí mismo, al buen nombre cuando afecta la reputación profesional o social y por último para el caso pertinente sobre datos personales que sea tratado como un dato más que puede identificar a la persona.

Esta característica de identificar a la persona se predica evidentemente del derecho a la imagen al representar aspectos del cuerpo. Su vulneración se hará cuando se tengan

tratamientos sin consentimiento o excediendo la finalidad inicialmente atribuida o evitando que puedan ejercerse derechos de actualización o corrección o con un filtrado masivo de información que se encuentra su imagen; en cualquier caso las circunstancias pueden resumirse en dos aspectos: falta de consentimiento en el uso de la imagen (principios de finalidad, de libertad, de transparencia, de legalidad) y ausencia de medidas técnicas de seguridad y el ejercicio de los derechos ARCO (principio de seguridad, principio de calidad, principio de veracidad, de confidencialidad, de acceso y circulación restringida)

Derechos integrantes del Habeas Data

Los derechos que integran el Habeas Data se denominan ARCARS: Autorizar el tratamiento, Rectificar los datos personales, Consultar los datos que conciernen, Actualizar los Datos, Revocar la autorización y Cancelar el tratamiento o uso de los datos.

La Corte Constitucional en sentencia C-748 de 2011 hace una enunciación bastante sucinta de estos derechos:

“Dentro de las prerrogativas o contenidos mínimos que se desprenden del derecho al habeas data encontramos por lo menos las siguientes: (i) el derecho de las personas a conocer –acceso- la información que sobre ellas están recogidas en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información; (ii) el derecho a incluir nuevos datos con el fin de [sic] provea una imagen completa del titular; (iii) el derecho a actualizar la información, es decir, a poner al día el contenido de dichas bases de datos; (iv) el derecho a que la información contenida en bases de datos sea rectificadas o corregidas, de tal manera que concuerde con la realidad; (v) el derecho a excluir información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa.

Derecho a Autorizar el tratamiento

Para garantizar la legalidad del tratamiento de datos personales es necesario contar con el consentimiento consciente y comprensivo de las personas. Ese consentimiento se manifiesta en la autorización de tratar los datos personales, después de entregados, con las finalidades y usos específicos que le comparte la política de tratamiento de información.

Esta autorización puede darse de manera independiente o dentro de las cláusulas de una relación jurídica más grande. En el primer caso tenemos cuando se aceptan las políticas de tratamiento de información y en el segundo cuando en el marco de la firma de una póliza, se autoriza a la compañía para que recolecte sobre nosotros toda información personal relacionada. Debe quedar constancia de esta autorización obtenida, no importa el medio.

El artículo 10° de la LEPDP establece los casos en que no procede exigir este derecho:

- “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. “

Derecho de Rectificación de los datos personales

Es un derecho cercano a la actualización, donde la persona busca que se modifique un dato que es falso o erróneo o que puede dar lugar a interpretaciones equivocadas de él como

persona. En cumplimiento de este derecho se encuentran el principio de veracidad o calidad del dato personal. A nivel internacional se conoce como habeas data rectificador.

Derecho de Consulta o Acceso

El derecho de acceso implica la posibilidad de que el titular pueda consultar y conocer toda la información personal que le concierne que se encuentra en la base de datos del responsable del tratamiento y además consultar que se estén tratando conforme a las políticas de tratamiento, de tal manera que la autorización no sea burlada. Puede hacerlo a través de dos puntos: haciendo la consulta directa al responsable o haciendo la petición a la SIC para que pueda conocer que bases de datos tienen información sobre él.

Este derecho es garantizado por el principio de transparencia en la administración de los datos personales. Se encuentra en los literales c y f del artículo 8 de la LEPDP, conocido como habeas data exhibitorio o habeas data finalista y artículo 4 del decreto 886 de 2014, este último se conoce como habeas data localizador en la doctrina internacional.

El artículo 11 de la LEPDP establece la obligación de suministrarle por cualquier medio legible la certificación de los datos personales que tenga almacenados el responsable, la finalidad para los cuales los tiene, cuales son los derechos que puede ejercer, quienes son los responsables y encargados del tratamiento.

Derecho de Actualización

Implica el derecho de que la persona incluya datos que reflejen la nueva situación personal y se cancelen o eliminen los anteriores, esto aplica para datos parciales, inexactos. Se encuentra en el literal a del artículo 8 de la LEPDP. Su ejercicio adecuado permite el respeto al buen nombre y cumple el principio de la caducidad del dato personal que ya no tiene relevancia

para la relación jurídica que estableció la finalidad. Adicionalmente también cumple el principio de calidad del dato. A nivel internacional se conoce como habeas data aditivo.

Derecho a Revocar la autorización

Este derecho es una facultad concedida al titular para hacer que se respete su voluntad en la autorización de tratamiento de datos personales. Los principios que garantiza este derecho son el de legalidad, el de la libertad.

En aras del principio de acceso y circulación restringida, seguridad y confidencialidad, el Titular tiene derecho a exigir que su información sea tratada de conformidad con los límites impuestos por la Ley y la Constitución y que en caso de incumplimiento existe un recurso efectivo para lograr el restablecimiento de sus derechos (ordinales a y d).” (Sentencia C-748 de 2011)

Derecho a la Cancelación o Supresión

Este derecho permite que el titular pueda eliminar aquellos datos irrelevantes para la finalidad del tratamiento de datos personales porque están desactualizados o son inexactos o generan una interpretación equivocada. A nivel internacional se conoce como habeas data cancelatorio. Este derecho es garantizado por los principios de libertad y legalidad del tratamiento

Algunos le denominan actualización de la información, es así como Corte lo define como el cumplimiento de unos presupuestos para cambiar el dato de la situación de la persona a la actual y eliminar el anterior, de cara a la idea que puedan hacerse otros (Sentencia T-157 Y T-164 de 1994) y no solo importa el criterio de veracidad; está prohibido el uso de bases de datos históricas. Si hay eliminación del dato se entiende que este se mezcla con el derecho de cancelación. Sin embargo dicha confusión ocurre porque al ejercicio de los derecho de actualización sucede el de rectificación de la información pues permite que se no se conserven

datos que luego sean utilizadas para perjudicar, al no contar ya con la autorización para tratar el dato irrelevante o cuya autorización ha sido cancelado.

Colisiones de derechos fundamentales

En algunos casos determinados el derecho a la protección de datos personales choca con otros derechos fundamentales como el de la vida, el de la información y el principio de la seguridad personal. En algunos de estos casos puede ceder y en otros imperar sobre ellos. Esto es posible debido a que pueden ser expandidos o reducidos su ámbito de aplicación, lo que se conoce como restricciones a los derechos fundamentales.

La solución que se tome cuando entre en conflicto dependerá siempre de los objetivos de interés general. Para discernir cuando es posible que pueda darse la restricción al respecto se ha visto adecuada la teoría de la ponderación, varios tribunales constitucionales del mundo la aplican con frecuencia.

Derecho al Habeas Data vs. Derecho a la información

Con respecto a la libertad de expresión y de información, sólo prevalecerá esta cuando la información deba ser conocida por el público, especial referencia se da con los casos de los políticos, directores ejecutivos de empresas y otros personajes, que en cierta medida sus actuaciones o su condición, hace que dependan de ella muchas personas y a raíz de ello deban tomar decisiones con la información más veraz y actual.

En el caso colombiano igualmente prevalece el derecho al Habeas Data sobre el de la información porque se encuentra inmerso en la dignidad humana (Sentencia T-414 de 1992, T-110 de 1993, T-577/92, T-486/92, T-022/93, T-164 de 1994) siempre que no sea para la satisfacción de un interés legítimo que reconoce el ordenamiento jurídico en cabeza del tercero

o pueda evitarse con ello la vulneración de derechos fundamentales como la intimidad, el buen nombre, el honor y la honra. Aquí la Corte hace una interpretación conjunta del artículo 15 y del 20 Superior.

Derecho al Habeas Data vs. Derecho a la salud

Cuando sea necesario salvar la vida de la persona, su integridad física o devolverle la salud y requiere del acceso a la información personal que se tiene en la historia clínica, el habeas data cederá en cuanto al principio de autorización, de supresión y de cancelación, pero se mantendrá el principio de finalidad para garantizar que los datos son tratados con miras a devolverle la vitalidad física y la protección de su dignidad humana.

La reglamentación europea (UE, 2016:10) trata acerca de la prioridad que tiene el derecho a la salud en cuanto que se logren los beneficios de las personas físicas y del sistema de salud en su conjunto. En este aspecto creemos que se refiere al uso de la información personal para lograr la gestión adecuada de ocurrencias, controles de calidad, la estadística de morbilidad y mortalidad y la investigación científica de las patologías que aquejan a las personas, todo sea para mejorar el sistema de salud.

Derecho al Habeas Data vs. Derecho a la vida

En los casos en que el tratamiento de datos personales sea necesario para proteger la integridad personal o la destrucción de la vida y la persona no pueda dar su autorización o ejercer su control como titular del dato podrá hacerlo cualquier otra persona, siempre que sea para lograr la preservación del derecho fundamental a la vida. En este caso de colisión hipotética prevalecen los principios de seguridad de la información, de finalidad y de temporalidad. Este sólo de manera inminente en que se ve amenazado el derecho a la vida de la persona y existe carencia para expresar un consentimiento consciente y pleno, es que cede el Habeas Data cede en su estricto sentido.

Derecho al Habeas Data vs. Seguridad Ciudadana

En este aspecto el conflicto ocurre cuando el Estado y sus organismos de inteligencia recopilan información personal y cuando se hacen simulaciones de vulneraciones al derecho fundamental con miras a fortalecer los sistemas de información.

En el primer caso, el Estado constantemente para garantizar la seguridad de los ciudadanos y el ejercicio de la soberanía, efectúa recopilaciones de datos sobre personas presuntamente envueltas en actividades delictivas. En esta colisión entre el Habeas Data y la seguridad nacional, prevalecerá esta última, en virtud de que es vital para cumplir objetivos que desarrollan los fines del estado: el interés general, el ejercicio de la soberanía, la protección de los ciudadanos y sus bienes; en conjunto representan un bien mayor frente al cual cede el interés jurídico de una sola persona

En la medida que sea necesario utilizar la información personal de cierta manera que implique una simulación de tratamientos indebidos de datos personales para garantizar la seguridad de la red, los servidores y la información almacenada que eviten un daño a la integridad, confidencialidad y autenticidad del tratamiento podrá permitirse, bajo estrictas medidas de cumplimiento y con aviso previo a las personas para que puedan entender que no se trata de una vulneración. Se busca impedir accesos no autorizados, distribución de software malicioso, ataques de denegación del servicio, interceptaciones en la transmisión electrónica de información entre las redes.

Nivel de Protección jurídica ante la vulneración del Habeas Data en Colombia, frente a los modelos europeo y norteamericano.

“Cuando se tiene el poder, se desea el predominio: si no se consigue (si todavía se es demasiado débil para ello), se desea la justicia, o sea un poder parejo”
Friedrich Nietzsche

La tecnología se ha metido en cada uno de los rincones, su principal función es de vigilancia y control a través de la recolección automática de datos personales, “(...) se procura información acerca de los individuos por todos los medios, en que se producen perfiles de las personas según sus comportamientos” (Brian, 2012:4), por este motivo los ordenamientos jurídicos reconocen un nuevo derecho fundamental: el de la protección o debido tratamiento de datos personales, cada uno de ellos ha seguido a algunos de los precursores (Estados Unidos y la Unión Europea) en el desarrollo de la tutela jurídica de este derecho.

Estos dos modelos han buscado regular una situación crecientemente preocupante: las transferencias internacionales de datos personales que representan una manera de escaparse a la tutela jurídica de los países con modelos fuertes para irse a lo que se denomina paraísos de datos, países que no tienen una regulación conocida que permite concluir un nivel de protección adecuado.

Las transferencias internacionales de datos personales se aceleraron por el uso del internet y las grandes posibilidades que abrió el big data, como una serie de procedimientos para extraer valor clave de la información que tienen las organizaciones públicas y privadas. Al respecto Remolina(2010b:376) menciona que los motivos de los gobiernos son variados: “(...)seguridad pública, seguridad nacional, investigaciones contra el terrorismo, labores de inteligencia militar o policial, cooperación judicial, cooperación internacional en general, protección de un interés del titular del dato, controles de inmigración”; a su vez las personas

privadas, sobre todo las empresas multinacionales, la requieren para planificar sus estrategias empresariales, atender a sus clientes en distintas partes del globo y sobre todo facilitar las economías de escala que permiten movilizar los recursos (el dato personal se cuenta como uno muy importante) allí donde sea más rentable analizarlo.

La Unión Europea ha sido la organización internacional más preocupada por obtener un nivel estándar mínimo de protección de los datos de las personas residentes en los países miembros. De hecho desarrolló dos documentos guía para evaluar el nivel de cumplimiento de la protección jurídica de las normas que son guía fundamental para el desarrollo a continuación de los requisitos que se solicitan y del análisis del grado de protección jurídica del régimen general de protección de datos personales de Colombia frente a las exigencias de la Unión Europea.

Estándares Internacionales aplicables al tratamiento de datos personales: Dos modelos de referencia

Existen dos modelos internacionales de protección de datos personales: modelo norteamericano y modelo europeo. El modelo norteamericano, o modelo sectorial, se centra en proferir normas sectoriales y dejar la autorregulación a las personas mediante códigos deontológicos y acuerdos contractuales; los países europeos guiados por la Unión Europea se centran en una norma constitucional fundamental, una ley general, una autoridad pública fuerte, es un modelo centralizado.

Tabla
 Dos Modelos de Protección de Datos personales²⁰⁶

Europa: Protección Datos Personales mediante estructura pública centralizada	EE.UU.: Privacy o regulación sectorial, con autonomía de cada persona para reclamar sus derechos a la privacidad vulnerados.
Normas constitucionales que reconocen un derecho fundamental al debido tratamiento de datos personales, unos principios comunes y su aplicación para personas de derecho público y privado.	Normas sectoriales para cada tipo de dato personal en intensidad proporcional a la afectación que ejerce sobre la intimidad o <i>privacy</i> .
Enfoque social orientado	Enfoque individualista
Derechos, principios comunes y excepciones en ley general	Los límites al tratamiento están en cada caso y tipo de dato. Algunos no se protegen porque priman intereses como la seguridad y la defensa nacional
Autoridad Pública Nacional	Algunas autoridades públicas por sector
Amplitud de la protección jurídica a través de diversos mecanismos	Limitación a las acciones civiles de responsabilidad.

Fuente: Camilo José Puello Rincón, 2016.

²⁰⁶ “En el derecho comparado existen dos modelos de protección de datos ampliamente reconocidos: un modelo centralizado y un modelo sectorial. El **modelo centralizado**, implementado en países europeos y, con algunas modificaciones, en la propia Unión Europea, parte de una categoría general de datos personales y de la idea de que cualquier tratamiento de ellos es considerado per se potencialmente problemático, razón por la cual debe sujetarse a unos principios y garantías mínimas comunes, susceptibles de ser complementadas con regulaciones especiales -según el tipo de dato y los intereses involucrados, pero que de ninguna manera suponen una derogación de los estándares de protección generales, que son aplicables tanto al sector público como al privado. Es propia de este modelo la existencia de una entidad central, autónoma e independiente, que supervisa la instrumentación, cumplimiento normativo y ejecución de los estándares de protección generales, y que está facultada para autorizar o prohibir las transferencias de datos internacionales atendiendo a la equivalencia de la protección que ofrece el país de destino.

En contraste, el **modelo sectorial** no parte de una categoría común de datos personales y por ello no se considera que todos estos datos deban estar sometidos a la misma regulación mínima, y por ello, bajo este modelo se adoptan regulaciones especiales y diferentes para cada tipo de dato personal, dependiendo de su relación con la intimidad –o privacidad como se denomina en el sistema anglosajón- y con la protección de intereses superiores –como la seguridad y la defensa nacional, es decir, la regulación sectorial se basa en una especie de ponderación de intereses que da lugar a reglas diferenciadas según el tipo de dato y que otorga más o menos poderes de intervención a las autoridades. En este modelo, la verificación del cumplimiento de las reglas también es asignada a autoridades sectoriales, que son dotadas de distintos poderes de vigilancia y control, según el nivel de intervención previsto por el legislador.”(Sentencia C-748 de 2011 MP Jorge Pretelt Chaljub)

Modelo europeo de protección de datos personales"

Los países europeos iniciaron una preocupación por el impacto de las tecnologías automatizadas de recolección de datos personales desde la época de la Segunda Guerra Mundial, donde el nacionalsocialismo contrató a la empresa IBM para el procesamiento de los datos que tenían almacenados y generar así un censo que ubicará a quienes fuesen judíos o tuviesen antecedentes (Remolina,2013:11). En este sentido esa época de horror representó un nuevo desafío para los ordenamientos porque el concepto de intimidad se había vulnerado definitivamente.

Conforme pasaron los años de la posguerra también fue disminuyendo los costos asociados al funcionamiento de las máquinas de cálculo – lo que serían nuestros modernos computadores - y aumentando el interés en su uso para procesamiento de la información que tenían las grandes empresas y el Estado. En este contexto entra en vigencia, sobre el año 1970, la primera ley sobre la materia: la *Datenschutz* del Land federal de Hesse en Alemania. Este mismo país adoptaría una Ley para todos los land en 1977 luego de que Suecia siguiese los pasos de Hesse al promulgar su ley en 1973. (Remolina, 2013:32)(Cerde, 2006)

Las características de estas leyes son 3: un registro público de las bases de datos de personas físicas recolectadas por medio automático, una autoridad de control que exigía el registro anterior y tiene facultades sancionatorias e inspectoras para el cumplimiento de la ley, por último le confieren facultades de información, acceso, rectificación, cancelación (Cerde Silva, 2006:223). Cabe resaltar que esto último será el germen de los modernos Derechos del Habeas Data que se denominan ARCO: Acceder, Rectificar, Cancelar u Oponer. Así como otros países europeos reconocen en sus constituciones el carácter fundamental del derecho de protección de datos personales entre los años 1970 a 2000.

La Comunidad Económica Europea expide el Convenio 108 en 1981 como normativa comunitaria que pusiera una estabilidad y generalidad común a los miembros para regular el todo lo relacionado con cualquier tipo procesamiento de datos personales por personas

jurídicas o naturales (ver el Artículo 1° del mismo y especialmente el capítulo II, parte que establece los principios que deben aplicarse). El compromiso fundamental fue adoptar los principios fundamentales del Convenio y crear sus propias normas estatales.

Importante destacar la Ley Federal alemana de 1990 que se expide porque tiene además del interés de adaptarse al marco del Convenio, se menciona la influencia de la sentencia proferida por el Tribunal Constitucional Alemán en 1982 mencionada en la sección anterior; es una sentencia que delimita jurídicamente el derecho a la autodeterminación informativa como independiente del derecho a la intimidad.

Las normas actuales que están vigentes en los ordenamientos jurídicos de cada uno de los países miembros de la Unión Europea se encuentran influidas por la Directiva 95/46/CE promulgada por el Parlamento Europeo y el Consejo Europeo; el status actual de esta regulación se obtiene a partir de la evolución inicial de las primeras normas sobre protección de datos personales que intentaron las autoridades nacionales y las autoridades comunitarias de Europa. Con esta directiva se logra una mayor vinculación de los ordenamientos nacionales para estandarizar todos bajo los mismos principios y mecanismos a efectos de estimular un mayor intercambio económico a partir del flujo seguro de datos personales. Finalmente el compromiso se fortalece con su reconocimiento en la Carta Europea de Derechos Fundamentales del año 2000 que fue aprobada por todos los miembros de la Unión Europea. Recientemente, el 27 de abril de 2016, fue expedido el Reglamento 2016/679 que deroga la Directiva 95/46/CE, sin embargo los conceptos emitidos en vigencia de la anterior norma europea siguen vigentes.

El modelo europeo de protección de datos personales tiene su eje sobre la concepción de derecho fundamental a la protección de datos personales, inicialmente parte del derecho a la intimidad. Es un modelo centralizado²⁰⁷ predominantemente porque existe una norma

²⁰⁷“Así, nivel de la Unión, (i) se prevén una serie de principios generales de obligatorio cumplimiento en todos los estados y aplicables a todo dato personal -salvo las excepciones señaladas expresamente, (ii) así como garantías para los interesados, como la notificación previa frente a la recolección y tratamiento de datos personales y el derecho a acceder y a oponerse al recaudo y circulación. Tales reglas garantizan niveles adecuados de protección, lo que a su vez facilita el flujo transfronterizo de datos.” Sentencia C-748 de 2011 MP Jorge Pretelt Chaljub MP Jorge Pretelt Chaljub. Así como una entidad central y pública que vigila el cumplimiento de (i) y (ii).

constitucional que reconoce la calidad de derecho fundamental, una norma general desarrollada, una autoridad pública de control y herramientas jurídicas para la protección.

En el sistema europeo se utilizan como sinónimos las expresiones “derecho a la protección de datos personales”, “Habeas Data” y “derecho a la autodeterminación informativa”. Bien se aprecia al observar la Carta Fundamental de derechos fundamentales en su artículo 8 que usa los vocablos de derecho a la protección de datos personales y la sentencia del tribunal constitucional alemán que lo define como “autodeterminación informativa”. El objeto de protección de este derecho fundamental es conservar el control de los datos personales, especialmente el uso y disposición de ellos sin vulnerar los principios que le conciernen a la persona de la dignidad, la autonomía y la inviolabilidad²⁰⁸.

Se consagran unos derechos del titular del dato y unos principios normativos informadores que irradian las normativas de los miembros de la Unión Europea. Actualmente el énfasis se pone sobre la manera para garantizar que se cumplan esos principios y se respeten los derechos al titular del dato personal.

Los europeos consagran dos grandes clases de mecanismos: tecnológicos y jurídicos. Los mecanismos tecnológicos se relacionan con las medidas humanas y técnicas que establecen a través del manual interno de procesamiento de datos personales; hay una vinculación a todos los que manejan los datos personales por encargo del responsable o del encargado. Esta clase de mecanismos no se enunciarán puesto que el grueso del análisis se centrará en los mecanismos jurídicos, que son la motivación de este trabajo de investigación.

Existen tres tipos de mecanismos jurídicos: tutela jurisdiccional, tutela administrativa y autorregulación.

Dentro de la tutela jurisdiccional se encuentran las acciones de protección de los derechos fundamentales, una acción específica en algunos países para proteger el derecho conocida como habeas data, la tutela penal a través de la tipificación de delitos informáticos

²⁰⁸En este sentido ver la obra de Carlos Santiago Nino *Ética y derechos humanos* publicada en 1989, páginas 199- 301.

por violación o tratamiento indebido de datos personales y por último la responsabilidad civil por daños causados.

Dentro de la tutela administrativa se resalta la Autoridad Nacional de Control que ejerce las facultades de inspección, vigilancia y control de las personas que traten datos personales por cualquier medio, técnico o mecánico, y facultades de promoción y educación en el derecho de protección de datos personales a todos los individuos. Otro mecanismo es el *Ombudsman* o defensor del pueblo, cuya principal facultad es la protección de los derechos fundamentales frente a la vulneración de las autoridades públicas.

En la autorregulación se tienen los códigos deontológicos que representan una forma vinculante de estandarizar en un sector económico la manera como se tratan los datos personales; los contratos acuerdo de transferencia de información, que imponen deberes contractuales entre las partes para permitir que se envíen datos personales; el encargado de la protección de datos²⁰⁹ o agente interno de protección, designado por el responsable del tratamiento de datos personales para que permita el ejercicio de los derechos ARCO mencionados anteriormente.

Modelo de Estados Unidos de América para la protección de datos personales"

El modelo estadounidense ha centrado su interés en promover regulaciones específicas o sectoriales del uso de los datos personales y la autorregulación de cada sector a través de las normas contractuales.

El mecanismo más común para proteger los derechos es mediante la utilización del *civil torts* - equivalente a la acción de responsabilidad civil colombiana.- Esta acción pretende obtener la reparación de daños causados.

²⁰⁹En el ordenamiento jurídico colombiano se denomina así a la entidad que finalmente termina tratando los datos por autorización del responsable del tratamiento de datos personales. Es adecuado no confundir, de ahí la necesidad de la presente aclaración.

Existe una diversidad de leyes de protección de datos personales, relacionados con la información pública (Privacy Act de 1974), la información escolar (Privacy School Act), sobre información financiera (Finance Privacy Act), por mencionar algunos ejemplos. Estas se centran en establecer los derechos de los individuos al acceso de sus datos personales almacenados.

El énfasis de la privacidad norteamericana es hacia el sujeto, quien tiene el derecho de resguardar su información en un lugar privado, no importa si es su hogar o si es un espacio donde normalmente accede el público. Desde que no sea la intención clara de que más personas se enteren, tendrá su derecho a la privacidad intacto y deberá ser respetado.

Sobre una descripción más detallada nos remitimos a los estudios que existen en Estados Unidos sobre el tema. Sin embargo a continuación se expone una breve descripción del modelo que hace la Corte Constitucional colombiana en sentencia C-748 de 2011, cuando analizó la constitucionalidad de la LEPDP:

“En contraste, el modelo sectorial no parte de una categoría común de datos personales y por ello no se considera que todos estos datos deban estar sometidos a la misma regulación mínima. Es por ello que bajo este modelo se adoptan regulaciones especiales y diferentes para cada tipo de dato personal, dependiendo de su relación con la intimidad –o privacidad como se denomina en el sistema anglosajón- y con la protección de intereses superiores –como la seguridad y la defensa nacional, es decir, la regulación sectorial se basa en una especie de ponderación de intereses que da lugar a reglas diferenciadas según el tipo de dato y que otorga más o menos poderes de intervención a las autoridades. La verificación del cumplimiento de las reglas también es asignada a autoridades sectoriales, las cuales son dotadas de distintos poderes de vigilancia y control, según el nivel de intervención previsto por el legislador.

Este modelo también se inspira en la idea de la autorregulación de los mercados, razón por la cual el Estado solamente participa en la protección de ciertos datos en ámbitos

en los que se presenta un alto riesgo de lesión de la intimidad, como la esfera financiera, la salud y los derechos de los niños.

Así, en Estados Unidos, aunque existe una ley federal de protección general de datos personales –*Privacy Act* de 1974 la regulación de los datos personales es regida principalmente por leyes sectoriales como la *Electronic Communications Privacy Act* (1986), que se relaciona con la protección de datos personales en comunicaciones electrónicas; la *Cable Communications Policy Act* (1994), que regula la protección de datos personales en archivos de televisión por cable; la *Fair Credit Reporting Act* - modificada de manera reiterada entre 1996 y 2001, que se refiere a los informes crediticios; la *Bank Secrecy Act* (1994), relativa a los registros bancarios; la *Telephone Consumer Privacy Act* (1994), sobre registros telefónicos; la *Drivers Privacy Protection Act* (1994), relacionada con la protección de los archivos de los permisos para conducir; la *Health Insurance Portability and Accountability Act* (1996), que regula la transferencia de seguros médicos; y la *Children’s Online Privacy Protection Act* (1998), sobre el control parental de los niños en sus actividades en Internet”

Principios comunes a las normativas y modelos internacionales

La importancia social que representan los nuevos datos personales, visto en el capítulo primero acerca del origen y desarrollo de la tutela jurídica del tratamiento debido de los datos personales como derecho fundamental y derecho humano autónomo, ha suscitado un espíritu de colaboración entre los dos modelos consonantes para acercar sus planteamientos normativos.

Esto ha influido en los países del mundo que han adoptado una mezcla de ambos modelos internacionales, interesados en obtener la aprobación del nivel de protección que exige cada uno de los modelos, cuando se realicen transferencias o recolecciones internacionales de datos personales desde Estados Unidos o alguno de los países miembros de la Unión Europea hacia sus territorios.

Algunos esfuerzos iniciales se vieron reflejados en la Resolución 45/95 del 14 de diciembre de 1990 sobre el establecimiento de principios generales para la reglamentación de ficheros computarizados. En esta relación se identifican que los países deben seguir los principios orientadores de:

- Legalidad y Lealtad: La información personal debe ser recolectada y tratada por métodos legales y acorde a los fines informados inicialmente al titular
- Exactitud: Los responsables de la información tienen el deber de comprobar, periódicamente o cuando los usen, que los datos guardados correspondan con la realidad y que además se conserven íntegramente.
- Especificación de la finalidad: La persona titular del dato personal debe ser informada del fin para lo cual se usarán los datos personales recolectados para ejercer un control de pertinencia, usos reservados al fin y temporal para cumplir el fin.
- Acceso de la persona interesada: Cualquier persona, que presuntamente cree que una base de datos guarda información de él, tiene derecho a saber si se procesa información que le concierne “(...) y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios. Debe preverse un recurso, en caso necesario, ante la autoridad supervisora especificada más abajo en el principio 8. El coste de cualquier rectificación será soportado por la persona responsable del archivo. Es conveniente que las disposiciones relacionadas con este principio se apliquen a todas las personas, sea cual sea su nacionalidad o lugar de residencia.”(ONU,1995:2) De este principio general se desprenden los principios de oposición y rectificación.
- No discriminación: “Sin perjuicio de los casos susceptibles de excepción restrictivamente contemplados en el principio 6, no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.”(ONU,1995:2)

- Excepción restringida: “Las excepciones a los principios 1 a 4 solamente pueden ser autorizadas en caso de que sean necesarias para proteger la seguridad nacional, el orden público, la salud pública o la moralidad, así como, entre otras cosas, los derechos y libertades de otros, especialmente de personas que estén perseguidas (cláusula humanitaria), 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. Las excepciones al principio 5, relativo a la prohibición de la discriminación, además de estar sujetas a las mismas salvaguardas que las prescritas para las excepciones a los principios 1 a 4, solamente podrán autorizarse dentro de los límites establecidos en la Carta Internacional de Derechos Humanos y en el resto de instrumentos aplicables en el campo de la protección de los derechos humanos y la prevención de la discriminación.”(ONU,1995:2)
- Seguridad: “Deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, como la pérdida o destrucción accidental, como humanos, como el acceso no autorizado, el uso fraudulento de los datos o la contaminación mediante virus informáticos”(ONU,1995:2)
- Supervisión y sanciones: “El derecho de cada país designará a la autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios arriba establecidos. Esta autoridad ofrecerá garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica. En caso de violación de lo dispuesto en la ley nacional que lleve a la práctica los principios anteriormente mencionados, deben contemplarse condenas penales u otras sanciones, junto con los recursos individuales adecuados” (ONU, 1995:2)
- Flujo transfronterizo de datos: “Cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos ofrezca salvaguardas similares para la protección de la intimidad, la información debe poder circular tan libremente como dentro de cada uno de los territorios afectados. En caso de que no existan salvaguardas recíprocas, no

deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que lo exija la protección de la intimidad” (ONU,1995:3)

- **Ámbito de aplicación:** “Los presentes principios deben hacerse aplicables, en primer lugar, a todos los archivos informatizados públicos y privados, así como, mediante extensión optativa y sujeta a los ajustes correspondientes, a los archivos manuales. Pueden dictarse disposiciones especiales, también optativas, para hacer aplicable la totalidad o parte de los principios a los archivos relativos a personas jurídicas, especialmente cuando contengan alguna información relativa a individuos.” (ONU, 1995:3)

Requisitos para un nivel adecuado de protección jurídica

La necesidad de recolección y transferencia internacional de datos personales “(...) exige que qué la transferencia se pueda realizar a un país con un adecuado nivel de protección” (Remolina, 2010a:493). Son reglas que en cierta manera no imponen un deber a los estados, que no hacen parte de los dos modelos internacionales de protección imperantes, sobre los cuales se ha hecho el consenso de modelos estándar, al ser los lugares donde han iniciado la revolución de las Tecnologías de la Información y las Comunicaciones, que mayoritariamente han adoptado para recibir los beneficios económicos de la instalación de negocios y competitividad²¹⁰. Esas reglas buscan evitar paraísos informáticos o *data havens*.

En cierta manera es un sello de confiabilidad frente a otros estados del mundo ser calificado como país con un nivel adecuado de protección jurídica y principalmente para las personas que habitan en el país al elevar los niveles de tutela jurídica de sus derechos fundamentales. Esto se conoce como “Principio de continuidad de la protección de datos” y significa una garantía que “(...) se ha establecido que para transferir datos de un país a otro se debe verificar que el país importador garantice un nivel “*adecuado*” de protección de datos

²¹⁰ El profesor Nelson Remolina (2010a:495) resalta que cumplir con el nivel de protección permitirá atraer las actividades son de las multinacionales. “En el plano empresarial, las multinacionales necesitan circular la información entre las diferentes sucursales o establecimientos que poseen en todo el planeta. Otras empresas requieren la información para brindar atención telefónica a los clientes por medio de call center, realizar acciones de mercadeo telefónico, (...) tener un perfil lo más completo posible sobre un potencial cliente, etc.”

personales. En este sentido, la expresión “*adecuado*” se refiere a que el Estado importador tenga un grado de protección superior, igual, similar o equivalente al del Estado exportador” (Remolina,2010a:497)

La resolución 45 de 1995 estableció el requisito para el flujo entre dos países de tener un nivel de protección jurídica semejante, le denomina “flujo transfronterizo de datos”. En la Directiva 95/46/CE se permite la transferencia si garantiza nivel de protección adecuado. Los factores para entender que es el nivel de protección adecuado son de índole regulatoria e instrumental (Cerde, 2011:337), que se deben fijar a partir los dictámenes que emite el grupo del artículo 29 de protección de datos personales de la Unión Europea. El profesor Nelson Remolina (2010a:500) explica que la regulación se refiere al contenido de las normas, que se refieran a los derechos del titular del dato y de los deberes del encargado o responsable del tratamiento y el factor instrumental a los mecanismos establecidos para su efectividad: judiciales o no judiciales, especialmente una autoridad pública de control.

La teoría de la *Privacy by design*, por ser ampliamente aceptada y producida a partir de los debates acerca de la protección de datos personales, es un insumo importante para considerar que un país ha incorporado en su ordenamiento jurídico y en su sociedad todo el conjunto de principios filosóficos y jurídicos que se predicen adecuados para la protección de datos personales

Adicionalmente a lo anterior se entra a analizar un tercer factor importante para asegurar que se cuente con la calificación de “adecuado” en el nivel de protección de datos personales. Este factor es la recolección internacional de datos personales, que surge a raíz de los desarrollos actuales de las TIC, de ciudadanos de cualquier país por empresas cuyo domicilio se encuentra en otro Estado que es posible que no cumpla con la normativa de protección, dejando a los ciudadanos sin poder ejercer sus derechos respectivos.

Desarrollo normativo

Para calificar de un desarrollo normativo se miran los tipos de normas expedidas. Al efecto en un análisis efectuado por el profesor Nelson Remolina se concluye que la mayor parte de los países que han recibido una calificación de “adecuado” han desarrollado normas de carácter constitucional, de carácter general y algunas sectoriales para datos personales específicos (Remolina,2010a :502)

Para analizar el contenido de dichas normas se toman los criterios propuestos por Cerda Silva (2006:227-234): ámbito de aplicación, principios informadores, derechos irrogados al titular del dato, las normas sobre responsabilidad de la materia y los mecanismos para la protección de los derechos del titular.

Ámbito de aplicación:

El marco europeo considera positivo la existencia de una norma que se aplique a todos los momentos de procesamiento y tratamiento de datos personales, incluyendo los que realizan privados y públicos o automatizados o mecánicos o manuales. Al respecto se refiere Cerda (2006:228) que es una técnica legislativa llamada *Omnibus*, que de aplicarse con rigidez evita las circunstancias específicas del tratamiento de datos personales, por esta razón que se han expedido regulaciones sectoriales para tener en cuenta los supuestos de hecho en que tiene el tratamiento de datos personales. Algunos ejemplos que trae Cerda Silva son para el sector de telecomunicaciones y el sector del trabajo con la selección de personal.

Para el caso específico colombiano debemos analizar la normativa existente y vigente en el ámbito general y en los sectores específicos. Al respecto este trabajo ya fue realizado por el profesor Nelson Remolina Angarita en un trabajo científico titulado “¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?”, publicado en el año 2010 por lo cual no nos referimos en la siguiente sección. Sin embargo

mencionaremos los criterios que se tienen en cuenta a manera de ilustración y por integralidad del régimen general de protección de datos personales.

Principios informativos:

Los principios informativos son un conjunto de enunciados normativos que tratan de homogeneizar los fundamentos jurídicos de todos los supuestos de hecho del procesamiento de datos personales en todos los ámbitos de aplicación. Una técnica *ómnibus* permite que existan principios normativos generales.

Los principios normativos que enuncia la Directiva 95/48/CE se relacionan con la estabilidad de las condiciones en el tratamiento, el almacenamiento y la importancia de informar al titular del dato personal; se mencionaron el de confidencialidad, seguridad, finalidad, consentimiento, calidad,(Ver supra.) Estos principios se encuentran inspirados en la teoría de la *Privacy by Design* que propende por proyectar más allá de los marcos jurídicos los principios de tratamiento de datos personales, en especial a la administración y la infraestructura de red y almacenamiento de datos personales de las empresas.

A su vez el profesor Nelson Remolina (2010a:501) expone en una tabla los principios que se tienen en cuenta dentro del análisis del cumplimiento de un nivel adecuado de protección jurídica.

Tabla 1
Principios mínimos que deben contener las regulaciones sobre
Protección de datos personales, según el estándar europeo

Principios básicos	Aspectos adicionales aplicables atipos especiales de tratamiento
Limitación de la finalidad	Datos sensibles
Calidad de los datos y proporcionalidad	Mercadeo directo
Transparencia	Decisión individual automatizada
Seguridad	
Acceso, rectificación y oposición	

Restricciones a las transferencias sucesivas a otros países	
---	--

Derechos del titular del dato personal

En la concepción moderna del derecho de protección de datos personales se da un papel activo a las personas con el otorgamiento de facultades amplias para retomar el control de sus datos personales. Se cuentan a partir de la Directiva europea con los mencionados derechos ARCO: acceso, rectificación, cancelación y oposición; representan facultades reconocidas a los sujetos para conocer la información que se tiene de ellos, conocer cómo se está utilizando y oponerse a la continuidad de su uso cuando se vulneren algunos de los principios normativos o los derechos conexos con este como el buen nombre, la honra, la imagen y la intimidad.

Brevemente se enuncia en qué consisten cada derecho debido a que fueron mencionados antes con gran detalle y conforme a varios autores, quedándonos con Cerda Silva como referente (al respecto ver Cerda Silva, 2006:232-233):

- Derecho de acceso: el titular le cuenten las operaciones del tratamiento, la finalidad y los intervinientes.
- Derecho de rectificación: Ejercido en el caso de que se almacenen datos personales que estén desfasados históricamente o no sean ciertos.
- Derecho de cancelación: Cuando la relación que permitió la recolección, que es en este caso la autorización y la finalidad, se termine el responsable debe aceptar la eliminación de los datos que tenga, así como evitar su uso posterior, aplica para los terceros que haya facilitado la información.
- Derecho de oposición: El derecho a ejercer una postura negativa ante el tratamiento de sus datos personales.

Responsabilidad por el tratamiento de datos personales

Este criterio se refiere a las sanciones que recaen sobre los responsables o encargados del tratamiento de datos personales; hay las sanciones administrativas y sanciones penales, por

otro lado existen las sanciones económicas por los daños causados que se responsabilizan a la entidad procesadora de datos personales.

Las sanciones administrativas las impone la autoridad administrativa de control de datos personales que vigila el cumplimiento de la normas y generan una multa de monto variable. Las sanciones penales crean tipos penales específicos que miran la afectación del bien jurídico y la culpabilidad(Cerda Silva,2006:233-234)

La responsabilidad es guiada por los dos tipos de responsabilidad que existen: objetiva y subjetiva; en el primer caso se tiene que responderá cuando ocurre el hecho dañoso sin importar el grado de control de él, en el segundo se mira la intención o imputación del hecho de indebido tratamiento al responsable.

Regulación de mecanismos de protección

De acuerdo con lo expuesto por el profesor Alberto Cerda Silva (2006:235) los mecanismos que establece la regulación europea son amplios y variados; son necesarios para garantizar el debido proceso a los sancionados como también la protección efectiva de los derechos vulnerados a los titulares de sus datos personales. El ejercicio comprensible de estos mecanismos permite que el cumplimiento sustancial de las normas repercuta en un respeto a la dignidad humana de cada persona.

Los mecanismos esenciales que garantizan un nivel de protección adecuado e impiden que los derechos vulnerados se queden sin protección efectiva son: control jurisdiccional, control administrativo y autorregulación.

El orden de mención se debe al grado proporcional de vinculatoriedad de cada mecanismo. Los controles jurisdiccionales son los preferidos porque permiten ejercer al titular del dato una reparación al daño causado que no se tiene en cuenta en los controles

administrativos²¹¹, pues aquí se sanciona es la violación de la ley con multas que van al fondo común de sostenimiento de la autoridad pública de control o de campañas que encabeza esta, según lo establezca la normatividad nacional. La autorregulación²¹² merece un caso aparte porque si bien puede generar un impacto social grande si trasciende a una regulación gremial, como los códigos de conducta, carece de lo que tienen los otros tipos de mecanismos como son la obligatoriedad del cumplimiento de la sanción por vulnerar el habeas data en el caso de que el sancionado se resista a ella.

Los mecanismos que encuentra Cerda Silva (2006) en el ordenamiento europeo son:

- Control jurisdiccional
- Autoridad Nacional de Protección de Datos Personales
- Defensor del Pueblo
- Agente de control Interno
- Códigos deontológicos

Control jurisdiccional

Dentro del control jurisdiccional se engloban todas las acciones procesales cuyo conocimiento está asignado al funcionario que ejerce jurisdicción en nombre del Estado: el juez. En Europa se encuentra el recurso de amparo, la acción de Habeas Data, la acción de responsabilidad civil, la acción penal, las medidas cautelares y la acción ejecutiva. Algunas de ellas serán de iniciativa del titular del dato, del sancionado o de la autoridad administrativa competente porque así lo dispone la ley.

Algunas legislaciones europeas contemplan un procedimiento específico, simplificado y concentrado que inicia desde la reclamación ante el responsable del tratamiento del dato personal, siguiendo luego con la queja a la autoridad administrativa y terminando ante el juez ante quien se interpone la acción judicial. Se le llama Habeas Data doctrinalmente.

²¹¹En el control administrativo se tiene la autoridad nacional de protección de datos personales y el defensor del pueblo.

²¹²Dentro de la autorregulación se tienen el agente de control interno, los códigos deontológicos

Autoridad Nacional de Protección de Datos Personales

La directiva europea le llama Autoridad de Control, su función es concientizar acerca de la normativa sobre tratamiento de datos personales, acompañar los procesos de adopción de políticas de tratamiento de datos personales por los encargados de hacer el tratamiento y de investigar o sancionar el incumplimiento de estos cuando son privados y, dependiendo de la norma, también a las entidades públicas.

El profesor Alberto Cerda (2006:244-246) agrupa las funciones conferidas así:

“1.- Difusión, Asistencia y Promoción. La autoridad de control es responsable de la difusión de las disposiciones legales y reglamentarias aplicables al tratamiento de datos personales, ya que las más de las veces la infracción a sus preceptos encuentra su explicación en una falta de conciencia de antijuricidad del comportamiento por parte del responsable de registros o bases de datos. A tal tarea se suma la asistencia a los más diversos sectores de la comunidad: a los titulares de datos, acogiendo sus denuncias y dándoles curso a través de un procedimiento de resolución alternativa de las controversias suscitadas entre éstos y las entidades tratantes de datos; a los responsables de registros y bases de datos, asistiéndolos en la formulación de códigos deontológicos, en la adopción de políticas de seguridad, entre otras; a los organismos públicos, informando las decisiones que recaigan sobre materias de su competencia. Además, la autoridad de control realiza acciones de promoción en la materia, por ejemplo, mediante la el fomento en la aplicación de tecnologías de protección de la intimidad por las entidades que procesan datos y la adopción de códigos de conducta por los responsables de tratamiento.

2.- Registro. La autoridad de control es responsable de un registro público de las entidades que tratan datos personales, las cuales deben practicar notificación previa a la iniciación de las operaciones de tratamiento, si bien se

admiten ciertas excepciones, por las cuales se releva o simplifica tal trámite, o bien se refuerza con exigencias adicionales, si es del caso. Además, en algunas legislaciones –es el caso de Francia y España– el registro se extiende a aquellos antecedentes que tienen relevancia general para una correcta aplicación e interpretación de la ley, tales como las resoluciones, informes o recomendaciones emitidas por la propia autoridad, así como los códigos de conducta que han merecido su aprobación.

3.- Inspección. La autoridad de control está dotada de facultades de inspección, las que incluyen el requerimiento de informes y antecedentes de los responsables de base o registros de datos, así como el ingreso y registro de los establecimientos y equipos en que se realizan las operaciones. Por su parte, los funcionarios de la autoridad de control quedan afectos a guardar confidencialidad con respecto a la información a que acceden con motivo del ejercicio de las facultades fiscalizadoras; y, en contrapartida, la obstrucción al desempeño fiscalizador –negativa a suministrar información, proporcionar información falsa y resistencia al acceso, entre otras– faculta a la autoridad para imponer sanciones de naturaleza administrativas a los responsables, o bien requerir su aplicación por tribunales.

4. - Facultades sancionadoras. La autoridad de control suele estar facultada para imponer sanciones administrativas –tales como multas y restricciones temporales para el tratamiento de datos– cada vez que se cerciora de la ocurrencia de actos u omisiones que importen una infracción a las disposiciones legales y reglamentarias vigentes, sin perjuicio de su reclamación judicial; si bien también existen algunas legislaciones que exigen un requerimiento judicial para tales efectos, como acontece en Suecia y Reino Unido. En cambio, tratándose de ilícitos de naturaleza penal asociados al tratamiento de datos, la autoridad de control sólo dispone de facultades procesales suficientes para seguir las acciones criminales del caso y obtener la sanción del infractor precisamente por los tribunales de justicia.

5.- Facultades cautelares. La autoridad de control por lo general dispone de facultades excepcionales para adoptar medidas cautelares –tales como decretar el cese temporal de las operaciones de tratamiento, el congelamiento de una base de datos, o el bloqueo de determinados datos– en casos graves en que exista un riesgo real o inminente para los derechos del titular de los datos personales.

6.- Facultades normativas. La autoridad de control dispone habitualmente de facultades normativas, ya sea de orden general, que se concreta en disposiciones reglamentarias, o bien particular, mediante la emisión de dictámenes u pronunciamientos específicos. Mediante tal expediente se concretan las previsiones generales de la ley, se orienta y conduce las operaciones de tratamiento de conformidad con los principios inspiradores de la ley, se salvan sus omisiones y hace frente a la obsolescencia normativa resultante de las permanentes innovaciones introducidas en el sector.

7.- Cooperación Internacional. La autoridad de control cuenta con facultades y atribuciones suficientes para practicar acciones de cooperación internacional en materia de tratamiento de datos, sea que ellas se dirijan hacia titulares de datos personales y entidades tratantes de datos con residencia en el extranjero, o bien hacia organismos internacionales o autoridades de control de otros países. Asimismo, tratándose de flujo transfronterizo de datos personales, la autoridad de control certifica que el nivel de protección brindado en otros países sea similar al brindado en nuestra legislación, y, de no ser así, autoriza en casos de excepción la transmisión de datos a tales países de destino.”

Agente de control interno

Es una persona que vigila el tratamiento de datos personales dentro de la organización responsable o encargada de hacerlo. La vigilancia que realiza se centra en el cumplimiento de las normas nacionales o europeas de protección de datos personales.

En la Directiva europea 95/46/CE se le denomina *encargado del tratamiento* y se aplica al que realicen las entidades públicas y privadas. Puede denominarse a esta persona más como un auditor, por su constante presencia, su conocimiento interno de la empresa y su especialidad. De esta manera se está más atento a los requerimientos iniciales de los titulares de datos personales, previniendo que se ahonden los problemas por indebido tratamiento.

Código Deontológico

Constituyen el intento de las asociaciones gremiales por adaptar la normativa general a los supuestos de hecho específicos que conllevan el tratamiento de datos personales que realizan, “(...) son una expresión de la autorregulación, por lo cual los propios agentes fijan normas para el desempeño de sus actividades (...)” y “(...) permiten hacer frente a la obsolescencia normativa y aún dirigir procesos normativos posteriores” (Cerda, 2006:238).

El profesor Alberto Cerda (2006:240-241) manifiesta que existen cuatro desventajas en el uso de estos códigos, que se reducen a dos, que se relacionan con su la participación y legitimidad de sus normas. El primer escollo es el de la inclusión de la mayor parte de perspectivas del sector o agremiación en la elaboración del código y el segundo se presenta respecto a la fuerza de cumplimiento a los mismos miembros y a los externos a la asociación, pero que pertenecen al sector.

Análisis del grado de protección jurídica de los mecanismos de protección frente a los estándares internacionales

En principio no se realizará un análisis del grado de protección jurídica de todos los requisitos para concluir si Colombia cuenta con un nivel de protección jurídica integral del derecho de protección de Habeas Data por dos razones: la primera se debe a que el desarrollo normativo el profesor Nelson Remolina desarrolló las directrices básicas para calificar el nivel de protección de la ley 1266 de 2008 y quedaría pendiente un análisis en la ley 1581 de 2012, que regula de manera general el derecho fundamental, sin embargo eso daría para algo diferente y más extenso que este trabajo de grado.

Ahora la segunda razón se debe a conservar finalmente los estrictos senderos demarcados al poner título de esta investigación, que son los mecanismos jurídicos, por ello se abandonará el análisis del nivel de cumplimiento de los presupuestos para una transferencia y recolección internacional de datos personales.

El documento de trabajo N° 4 de 1997 que establece unas orientaciones básicas acerca de lo que entiende “nivel adecuado” de protección de datos personales no estableció un procedimiento específico de análisis para realizar esta valoración. Sin embargo fijó los objetivos que debe cumplir cualquier sistema para que pueda ser catalogado con este nivel (UE, 1997b:7):

“1) Ofrecer un **nivel satisfactorio de cumplimiento** de las normas. (Ningún sistema puede garantizar el 100 % de cumplimiento, pero algunos son mejores que otros). Un buen sistema se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo es, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos.

2) Ofrecer **apoyo y asistencia a los interesados** en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.

3) Ofrecer **vías adecuadas de recurso** a quienes resulten perjudicados en el caso de que no se observen las normas. Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.”

Como se mencionó anteriormente en el aparte “Colisión de derechos fundamentales” en la situación actual uno de los conflictos que se presentan es entre el derecho a la información y el derecho al debido tratamiento de datos personales.

Como bien se ha afirmado a lo largo de este trabajo el Habeas Data entra en colisión con otros intereses importantes para el ejercicio de la política pública y del desarrollo económico. Si bien ha cedido parte de la restricción absoluta de tratamiento de datos personales, hasta llegar al núcleo esencial de ese derecho, debe valorarse ahora en que medida las herramientas jurídicas son el muro de contención para evitar que el ejercicio de la libre empresa económica y del desarrollo de los fines del Estado extingan la llama del habeas data, con ella los derechos del buen nombre, del olvido, del honor, de la imagen, en fin, de la dignidad del hombre como ser autónomo en el ejercicio de configuración de su vida.

Analizados los criterios definidos anteriormente por el grupo de trabajo del artículo 29 de la directiva se puede afirmar que Colombia a nivel de los criterios cumple parcialmente. En ese sentido se establecieron recursos administrativos y judiciales de manera explícita para sancionar la violación de la ley a través de un delito y una falta a la norma, de esta manera se esta cumpliendo parcialmente con el criterio número 3. Sin embargo se deja por fuera los aspectos concernientes a la indemnización por los daños causados, que debería estar en un régimen propio de responsabilidad civil por indebido tratamiento de datos personales, de esta

manera se evitaría recurrir por analogía a los principios establecidos para la responsabilidad civil contractual y extracontractual. Esto es algo que contempla la Corte Constitucional colombiana en su sentencia C-748 de 2011 que le llama “principio de indemnización”, mencionado supra en los principios jurisprudenciales desarrollados.

El criterio número 2 es el único perfectamente cumplido, pues existe una institucionalidad que se encarga de supervisar, vigilar y controlar el cumplimiento adecuado de las normas de protección de datos personales. Se establecen unos términos para que los titulares del dato reciban respuesta de los encargados y responsables del tratamiento, se fija la competencia para iniciar investigaciones rápidas que permitan definir la violación del derecho de protección de datos personales.

En cuanto al criterio número uno sobre el nivel satisfactorio de cumplimiento, pasamos a plantear preliminarmente algunas problemáticas encontradas que pueden generar una falta de efectividad de las herramientas jurídicas por ausencia de protección de derechos del habeas data correspondiente a los datos personales exceptuados de la aplicación de la LEPDP y por inadecuado diseño de la misma herramienta.

Algunas problemáticas identificadas en las herramientas jurídicas

a) Ausencia de principios rectores importantes

La Ley Estatutaria de Protección de Datos Personales (LEPDP) de Colombia reconoce algunos principios que fundamentan el derecho de la protección de datos, reconocidos a nivel internacional. Los más importantes los ha incorporado al ordenamiento jurídico: el principio de legalidad, de finalidad, de libertad, de veracidad, de transparencia y de acceso y circulación restringida.

El principio de legalidad permite que se proteja la confianza legítima de las personas en que sus datos se tratarán con un marco definido a partir del que puedan reclamar su incumplimiento.

El de finalidad incluye los principios internacionales de finalidad en sentido estricto y de limitaciones en el uso, retención y divulgación, evita que pueda ser asediado en sus datos por otras empresas a los cuales no dio su información, pero que le fue transmitida.

El principio de libertad, es el equivalente del principio de consentimiento, si faltase este principio simplemente ya se tendría un indebido tratamiento de datos personales, aunque posteriormente puede ser legitimado por medio de la solicitud de autorización al titular, pero esto no obsta de responder por las consecuencias que trajo la violación de la ley hasta cuando obtuvo el consentimiento.

El principio de transparencia permite a las personas ejercer en plenitud sus derechos ARCO y es el soporte indispensable para el ejercicio de las herramientas jurídicas que consagró el ordenamiento jurídico y que fueron estudiadas en la sección anterior (*supra* Herramientas jurídicas para la protección de datos personales).

Se echa en falta la consagración como principios rectores de los principios de precisión, de límites en la recolección y el de rendición de cuentas. Ciertamente el de precisión es tratado como de calidad y veracidad del dato, pero se cree que es más adecuado el uso del concepto de precisión porque hace recaer la obligación de conservar los datos fidedignos para la finalidad establecida; en cuanto a los límites de recolección, la ley señala expresamente algunos datos personales que no pueden ser tratados, pero no hay una prohibición absoluta en el tratamiento de ellos, pues pueden hacerse siempre que exista consentimiento, una grave situación que puede prestarse a posibles vulneraciones si no se cumple el principio de seguridad, sobre todo si tenemos en cuenta que algunas bases de datos sensibles son de personas que no podrían ejercer fácilmente el acceso a lo que se sabe de ellos; sobre la rendición de cuentas, esta se une junto al principio de acceso y el de apertura en uno llamado transparencia, dejándolo a voluntad de la persona que entregó sus datos personales el ejercicio y no como obligación propia del encargado del tratamiento.

Falta un nivel de protección adecuado, que este acorde a las necesidades de aplicación de los principios de administración y tratamiento de datos personales de acuerdo al tipo de

dato personal que se recolecta. Para ello podría ser aplicable la teoría de la *Privacy by Design (PbD)* que establece la necesidad de unos parámetros técnicos para incluirse en tres aspectos clave de los responsables y encargados del tratamiento de datos personales: tecnología, prácticas del negocio y el diseño físico.

Adicionalmente reforzarían el régimen de protección de datos personales que se hubiesen incorporado el principio “pro homine”, pues permite que se le conciba como ser humano con una dignidad inherente, impidiendo que se le tenga por simple contenedor de información, que es útil en la medida que entregue información personal para ofrecerle mejores productos, dejándolo ignorante de los procesos de tratamiento que se realizan entre el momento que recolecta la información y la entrega de los servicios y productos. Si bien este principio se encuentra establecido en la Constitución, se cree que al ser una actividad reglada y en cumplimiento del principio de legalidad del tratamiento debió incluirse dentro de la LEPDP.

b) Autonomía de la autoridad pública de control

El ejercicio de la facultad de Autoridad de Protección de Datos personales es delegado a un Superintendente para la protección de datos personales, que depende y es nombrado por el máximo responsable de la Superintendencia de Industria y Comercio. Esta falta de autonomía es una situación problemática respecto al tema de la autonomía y la capacidad financiera.

Estos dos aspectos incidirán en el cumplimiento de los deberes asignados a la entidad para la inspección y vigilancia de los encargados y responsables. Especialmente en el cumplimiento de la socialización del régimen y de las orientaciones en la aplicación de la LEPDP.

- c) Ausencia de leyes estatutarias sectoriales para los datos exceptuados de la aplicación mayoritaria de la LEPDP.

La ausencia de leyes especiales que regulen los datos exceptuados de la aplicación de la ley estatutaria de protección de datos personales (LEPDP) representa una inseguridad jurídica al momento de aplicar el cumplimiento de las normas sobre tratamiento de datos personales. Si bien aplican los principios generales de la misma no es así en cuanto a los derechos, obligaciones de los encargados y las herramientas específicas diseñadas para una protección.

La Corte Constitucional en sentencia C-748 de 2011 llamo al legislador a regular la protección de esos datos personales exceptuados de la aplicación de la mayor parte de la LEPDP. Hasta el momento no han sido proferidas normativas especiales para ello.

Por esta razón los datos sobre salud, relaciones laborales, datos de niñas, niños y adolescentes junto a los datos recabados en actividades electorales se encuentran un poco desprotegidos. Esto le resta oportunidades económicas importantes para el país en cuanto al turismo de servicios de salud, de call centers que atiendan pacientes de otros países, entre otras oportunidades.

- d) Medida cautelar por una autoridad administrativa

Las medidas cautelares solo pueden ser decretadas por una autoridad judicial o una autoridad administrativa cuando actúa con funciones jurisdiccionales. Más sin embargo, remitámonos al CPACA, para encontrar la norma que pueda posibilitar el decreto de medidas cautelares en procesos administrativos sancionatorios.

En el artículo 20 del CPACA, su segundo inciso se establece la autoridad podrá adoptar la medida solicitada cuando este en peligro la integridad personal o la vida del solicitante. Esto en cuanto al régimen del derecho de petición regulado en la ley 1755 de 2015. Sin embargo la

competencia de la autoridad se limita a la relación que exista entre la medida solicitada y la guarda del derecho, quizá no se entienda como una medida cautelar, sino más bien como una respuesta al deber constitucional de guardar la integridad de todos los ciudadanos.

En el artículo 47 del CPACA que regula todo el trámite del procedimiento administrativo sancionatorio no se establece la existencia de decretar medida cautelar alguna. Y si se hace referencia a la competencia para hacerlo, está se encuentra únicamente en cabeza de los jueces de lo contencioso administrativo y por ello se encuentra en la parte segunda, que que regula todo lo relacionado con la jurisdicción contenciosa administrativa.

La medida cautelar de bloqueo temporal de los datos es inconstitucional porque rompe con la división funcional de los poderes públicos al asignar facultades de exclusivo resorte de un juez de la república y no de una autoridad pública que ejerce facultades administrativas, lo cual vicia todo procedimiento donde se decrete esta medida al quebrantar la Constitución Política. Por ello falta regular con mayor claridad el procedimiento y las consecuencias de la facultad de decretar la medida cautelar de bloqueo de datos concedida a una autoridad administrativa como es la Superintendencia de Industria y Comercio.

La Corte Constitucional concibe las medidas cautelares como un instrumento necesario para proteger provisionalmente un derecho mientras dura un proceso, para garantizar que al final se cumpla la decisión. En sentencia C-379 de 2004 confirmó la naturaleza jurisdiccional de este instrumento al decir que:

Las medidas cautelares tienen amplio sustento constitucional, puesto que desarrollan el principio de eficacia de la administración de justicia, son un elemento integrante del derecho de todas las personas a acceder a la administración de justicia y contribuyen a la igualdad procesal.

La medida cautelar de bloqueo temporal de datos personales es un instrumento inconstitucional, cabría solicitar la excepción de inconstitucionalidad cuando la decrete en un procedimiento administrativo la Superintendencia de Industria y Comercio.

e) Protección del titular del dato personal las normas corporativas vinculantes

La protección del titular del dato personal en el caso de las normas corporativas se presenta como una problemática mayor cuanto que no es parte en las normas corporativas vinculantes que se pactan entre grupos de responsables y encargados del tratamiento.

Es un problema latente y que podría agravarse si no se presenta la regulación gubernamental que fue encargada al gobierno nacional por medio de la LEPDP.

Tres puntos principales son los que debe tocar la regulación específica del posible decreto que expida el Gobierno sobre normas corporativas vinculantes:

- Los procedimientos para realizar el reclamo de los derechos ARCO o ARCARS
- La exigencia de las normas corporativas vinculantes ante los recursos y herramientas jurídicas.
- La obligatoriedad de indemnización por daños causados en el tratamiento de datos personales.

CONCLUSIONES Y RECOMENDACIONES

El derecho a la intimidad se concibe como un espacio reservado, donde el individuo puede desarrollar sus propias expresiones sin el temor de que puedan acceder sin permiso las personas para conocer de ellas. Por este motivo se afirma que el derecho a la intimidad surge del principio general de la libertad porque permite el despliegue de la personalidad y es una de las limitaciones de la actividad estatal y particular en la vida de cada persona y la afirmación del individuo como ser capaz de autonomía. Está profundamente conectado con la dignidad humana como garantía, principio y valor para el soporte de los derechos humanos.

La concepción negativa de la intimidad o privacidad está vinculada a los contextos histórico-jurídicos de la escuela del derecho racional y el liberalismo, que impulsaban la limitación de la actividad estatal a través de la formulación de posiciones jurídicas que debían ser respetadas porque le permiten a cada persona desarrollar su personalidad en plenitud. Esta concepción se compone de tres elementos: un espacio ideal reservado, expresiones propias del individuo, desconocidas para la mayoría de las personas.

Sin embargo las tecnologías de la información y la comunicación impactan profundamente en esta concepción introspectiva del derecho a la intimidad. El dato personal crece en su importancia por lo que puede hacerse con él gracias a las tecnologías de tratamiento y análisis de información que se han creado. Los datos personales según la accesabilidad se clasifican en aquellos que pueden conocer la mayor parte de las personas, aquellos que solo conciernen a nuestra persona y familiares, otros que conciernen a personas que tienen cierta cercanía o vínculo jurídico, por último existen datos privados que sólo deben tratarse con discreción como los que expresan nuestro origen racial, nuestras opiniones políticas o nuestra pertenencia a sindicatos.

El uso tecnológico del Dato Personal representa una nueva fuente de crecimiento empresarial, innovación e incertidumbre. Es una fuente de crecimiento empresarial debido a que los servicios tecnológicos lo usan como materia prima para tener mayor rentabilidad al

satisfacer mejor con sus servicios las necesidades de las personas. Es una fuente de innovación porque permite generar nuevos productos o servicios que encajan con las necesidades de las personas. Es una fuente de incertidumbre porque en su actividad empresarial, lucrativa e innovadora se puede vulnerar el derecho fundamental de la libertad, del buen nombre, la honra, el honor o la integridad personal; derechos de la personalidad que pueden ser desconocidos si sólo se mira el dato personal como información y no la actividad de tratamiento de ellos por terceras personas como un poder vigilante que trata de conocer cada pequeña parte de nuestra vida.

Ante este riesgo potencial que representa el uso de la tecnología para los derechos de la personalidad por la falta de tutela jurídica, se incluye en la concepción introspectiva de la intimidad, la proyección social de la persona que genera datos personales. Posteriormente esa protección es independizada del derecho a la intimidad como un nuevo derecho fundamental que llaman autodeterminación informática, habeas data o tratamiento debido de datos personales.

La necesidad de equilibrar la balanza frente al poder informático hace necesaria inclusión de la proyección social como una nueva faceta del derecho a la intimidad que no niega la intromisión en la vida privada y da una facultad jurídica a las personas para controlar el uso de los datos y evitar o evidenciar las violaciones producidas.

La importancia de las herramientas jurídicas, sean jurisdiccionales o administrativas, para proteger los derechos fundamentales conexos al tratamiento de los datos personales genera la total independencia de la faceta activa del derecho a la intimidad como un nuevo derecho para hacer efectivo al control y supervisión de los sujetos que realizan tratamiento, dentro de unos estándares o principios reconocidos internacionalmente.

El desarrollo de nuevos derechos fundamentales se ha apoyado en la constitucionalización del derecho y la concepción generacional de los derechos humanos.

La constitucionalización del derecho es una garantía de protección que tiene el ciudadano frente al Estado y los particulares, al orientar su actuar al reconocimiento y protección efectivo de posiciones jurídicas de interés para las personas, a través de unas funciones y procedimientos jurisdiccionales o administrativos fijados en un texto normativo superior a todo el ordenamiento vigente. Esto representa un aumento de la importancia de la dimensión normativa de los derechos fundamentales al punto de convertirlas en normas imperativas de cumplimiento estricto para todos, sin necesidad de esperar un desarrollo concreto normativo y funcionando como orientadoras de las que existen en cada rama del derecho.

La concepción generacional concibe el surgimiento de nuevos derechos según las necesidades humanas históricas, que claman por instrumentos de protección, esto sucede con el habeas data que pertenece a la llamada *tercera generación* de derechos que protegen las libertades de la primera generación de cualquier “contaminación”.

El derecho de la protección de datos personas es una nueva rama del derecho que se encarga de estudiar la faceta sustancial y procesal del derecho fundamental. Tuvo un desarrollo histórico a lo largo del siglo XX, lo que llevo finalmente a una ola de reconocimientos jurídicos como norma iusfundamental comenzando con la Ley Fundamental de Alemania, la Constitución de España y la de Portugal; posteriormente le siguen otros países europeos y latinoamericanos. Los países latinoamericanos han regulado el fenómeno del tratamiento de datos personales de múltiples maneras, bien sea reconociendo algunas de sus faceta procesal o sustancial o ambas, todos los ordenamientos jurídicos consagran una norma constitucional para regularlo.

La faceta sustancial concierne derechos de control y revisión del tratamiento de los datos personales que nos conciernen, de las obligaciones y cargas que se asignan a los sujetos tratantes de datos personales, de los tipos de dato personal y las excepciones o prohibiciones al tratamiento de ellos. La faceta procesal corresponde al conjunto de mecanismos judiciales o administrativos que protegen los derechos principales y conexos.

El reconocimiento y desarrollo jurisprudencial de nuevos derechos ha sido posible en Colombia por la adopción del modelo de Estado Social y Constitucional de Derecho en la constitución de 1991, en esta se reconoció el derecho fundamental a la intimidad y un nuevo derecho de habeas data o de protección de datos personales. En esto ha tenido un gran papel la jurisprudencia constitucional al garantizar la efectividad de la Constitución y el impulso al órgano legislativo para que legisle. En ausencia de norma que dé expreso desarrollo legal estatutario a sus contenidos esenciales y herramientas jurídicas, la Corte Constitucional colombiana desarrolló estos derechos por medio de la acción de tutela.

A través del desarrollo jurisprudencial de la Corte Constitucional colombiana el Habeas Data pasó por cuatro fases claras: como garantía del derecho a la intimidad y la libertad, como derecho a la autodeterminación informativa, derecho de protección de datos personales y derecho al debido tratamiento de datos personales. Esta última fase afirma que el Habeas Data es un derecho instrumental con doble faz: una sustancial y otra procesal.

El Derecho al debido tratamiento de datos personales es un derecho fundamental de limitación del tratamiento dentro de unos parámetros constitucionales y otorga una serie de facultades para garantizar la vigilancia del cumplimiento.

El derecho fundamental al debido tratamiento de datos personales da a las personas la capacidad de exigir a las administradoras de datos personales el acceso, inclusión, exclusión, corrección, adición, actualización, y certificación de los datos, así como la limitación en la posibilidades de divulgación, publicación o cesión de los mismos, conforme a los principios que informan el proceso de administración de bases de datos personales. Son conocidos como derechos ARCO. El tratamiento o administración de datos personales es un conjunto de prácticas que las entidades públicas o privadas adelantan con el fin de conformar, organizar y depurar bases de datos personales; la actividad de administración de datos personales debe regularse por los principios de libertad, consentimiento informado, necesidad, veracidad, transparencia, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad.

En el mundo el tratamiento del Habeas Data destacan las legislaciones de Estados

Unidos y la Unión Europea, las cuales se convirtieron en modelos a seguir para regular todo lo relacionado con el tratamiento de datos personales. Algunos países combinan ambos modelos como Colombia.

El modelo europeo se centra darle una importancia constitucional, crear herramientas jurídicas de naturaleza administrativa y jurisdiccional así como también crear una autoridad pública de control en los distintos niveles territoriales para garantizar el cumplimiento. El modelo estadounidense es autorregulatorio, no reconoce el Habeas Data como derecho independiente y lo incluye como parte de la intimidad o *privacy*, es protegido a través de múltiples leyes sectoriales que crean autoridades de control públicas para cada sector económico según el tipo de dato personal regulado y solo conceden acciones de responsabilidad civil por daños a la persona que desee reclamar el incumplimiento.

En los ordenamientos de los países latinoamericanos existen muchos tipos de habeas data debido a la diversa finalidad que cumplen, el momento en que se puede iniciar su acción, los efectos de la sentencia y el tipo de legitimación por activa que reconoce. Esto permite tener un rico panorama acerca de las mejores experiencias en la región frente a las herramientas creadas, sin embargo Colombia se basó exclusivamente en algunas partes del modelo europeo de protección de datos por lo cual el legislador en su proyecto de ley aprobado se olvidó de algunas herramientas jurídicas: régimen propio de responsabilidad civil para datos personales, la creación de algunos tipos penales más especializados, la definición de competencias más especializadas y centralizadas de la Superintendencia de Industria y Comercio frente a las conductas violatorias del habeas data por las entidades públicas, la creación de códigos de autorregulación válidos y el desarrollo legal y no reglamentario de las normas corporativas vinculantes pues hasta el momento hay en este último tema un caso de anomia.

Estos modelos comparten algunos principios como el de Legalidad y lealtad, exactitud del dato, especificación de la finalidad, acceso de la persona interesada, no discriminación, excepción de tratamiento restringido, seguridad del dato, supervisión y sanciones, flujo transfronterizo seguro y ámbito de aplicación. Estos principios comunes a ambos modelos son un intento de la ONU por acercar ambos.

En Colombia hay una diversidad de herramientas jurídicas, algunas reguladas explícitamente para la protección del derecho fundamental del habeas data, pero la mayoría aplicadas por analogía dado la pretensión que se busca. Las herramientas jurídicas que existen en Colombia reguladas específicamente son de índole administrativa: una modalidad del derecho de petición (reclamo, queja), una autoridad administrativa de control, contractual: política de tratamiento de datos personales y normas corporativas vinculantes. Sin embargo no se omiten las acciones judiciales que protegen derechos fundamentales (acción de tutela), bienes jurídicos que pueden ser lesionados o puestos en peligro (tipos penales informáticos), intereses jurídicos perjudicados por el indebido tratamiento (responsabilidad civil) o el incumplimiento de las obligaciones en un contrato (acción ejecutiva para normas corporativas vinculantes).

El reclamo y la queja son una modalidad del derecho de petición porque sus objetivos son pedir que se realice algo: una que establece el derecho de pedir información de datos personales, que se corrija la información personal o que se retiren de la base de datos. Es procedente para consultar la información, pedir que se cumplan las normas del régimen general de protección y obligar a que se respeten otros derechos constitucionales vulnerados por medio del tratamiento indebido de datos personales.

La Superintendencia de Industria y Comercio estableció una tipología muy clara de los reclamos que deben reportar los operadores de información de la ley 1266 de 2008. Esta tipología es útil para comprender fácilmente los tipos de reclamaciones que se presentan para la protección de datos personales en el régimen general.

La acción de tutela para proteger el debido tratamiento de datos personales sólo procede subsidiariamente, cuando haya una inminente violación de este derecho, esto se manifiesta ante la renuencia del sujeto tratante del dato personal o la demostración de perjuicios sobrevinientes si se procede a utilizar cualquiera de las otras herramientas jurídicas establecidas. Se ha convertido en el mecanismo más importante para asumir que la Constitución debe seguir siendo vinculante, la Corte Constitucional da un ejemplo de juez

garantista en medio de una sociedad profundamente desigualitaria no sólo en los aspectos económicos sino educativos.

La acción de responsabilidad civil por indebido tratamiento de datos personales debe remitirse al régimen general de responsabilidad que establece el Código Civil colombiano. De acuerdo a los supuestos de este la responsabilidad civil se genera ante el hecho ilícito que consiste bien en el incumplimiento de la política de tratamiento de datos personales o bien en el uso sin consentimiento informado de los datos personales, adicionalmente que debe surgir subsiguientemente el daño causado a raíz de cualquiera de los anteriores supuestos anteriores.

Las conductas de tratamiento indebido de datos personales son: i) una intrusión sin permiso en la base de datos, ii) la alteración o entrega de la base de datos por parte de los dependientes del responsable o encargado, iii) el engaño o fraude para obtención de los datos y tratamiento de datos personales.

Se recomienda en una futura legislación específica sobre responsabilidad civil en el Habeas Data que opte por un régimen de responsabilidad civil objetiva y solidaria entre las partes tratantes de información por causa de esta, dado que se enmarca por lo menos en una actividad contractual y colaborativa, que tiende a un resultado en virtud del principio de finalidad y en el caso de extracontractual una obligación de diligencia y cuidado en la actividad potencialmente peligrosa que entraña el tratamiento de datos personales por las consecuencias del poder informático indebidamente usado.

Por lo anterior queda el reto de encarar a futuro una investigación sobre el régimen de responsabilidad civil por indebido tratamiento de datos personales en Colombia a partir de estas pinceladas realizadas.

La acción penal es procedente como herramienta jurídica de protección siempre que se cometan algunos de los delitos creados por la ley 1273 2009. Esta ley es una reacción al fenómeno criminológico de la cibercriminalidad como intento para controlar la afectación de la confianza legítima de las personas en la tecnología a raíz del uso de esta para cometer

conductas perjudiciales de los intereses patrimoniales. Los tipos penales creados se caracterizan por ser de peligro y en blanco dado el potencial riesgo que representan las actividades informáticas para las personas y la necesidad de dejar cierta flexibilidad para que pueda ajustarse el delito a la rápida evolución de conceptos en la informática. Los bienes jurídicos protegidos son la seguridad de la información y la seguridad de los sistemas informáticos, en los primeros se protege el acceso seguro de la información de ataques realizados con técnicas avanzadas, los segundos se protege el normal funcionamiento de lo que respalda la disponibilidad de información.

A través de la acción penal por violación o puesta en peligro de los bienes jurídicos aludidos se busca garantizar los principios de calidad, consentimiento informado, confidencialidad, seguridad y acceso restringido a la información personal, con ellos se castiga toda conducta que pretenda rebajar obtener un beneficio a costa de estimular el miedo al uso de las TIC.

La tutela administrativa es una de las herramientas por medio de la cual el Estado ejerce su función de promoción y protección de los derechos fundamentales. En el régimen de protección de datos personales el estado la ejerce a través de su poder sancionador y su poder de policía administrativa. Hay una diversidad de entidades que ejercen alguna o todas las funciones encomendadas al prototipo ideal de autoridad de protección de datos personales. Esto complica el panorama en la supervisión del cumplimiento de las normas de protección de datos personales así como en la función de sanción al presentarse un potencial conflicto de competencias administrativas entre las entidades públicas ante un conflicto positivo de competencias administrativas.

Pese a la diversidad de entidades que actúan en el régimen general de protección de datos hubo un acuerdo y sus actuaciones sancionatorias deben realizarse mediante el procedimiento especial que trajo la ley 1438 de 2011 y en términos constitucionales aplican las normas sobre el debido proceso: legalidad, tipicidad previa a la conducta sancionada, proporcionalidad en la medida de la sanción y procedimiento claro y seguido. Este

procedimiento administrativo puede iniciarse a petición de parte por medio de la queja o el reclamo o de manera oficiosa.

Dentro de las facultades otorgadas a la Superintendencia de Industria y Comercio, como Autoridad de Protección de Datos Personales, la medida cautelar de bloqueo temporal de datos es una medida inconstitucional porque es exclusivo resorte de un juez de la república y no de una autoridad pública que ejerce facultades administrativas, lo cual vicia todo procedimiento, que indaga ante una posible infracción en el cumplimiento de las normas de protección de datos personales, donde se decreta esta medida al quebrantar la Constitución Política. Por ello falta regular con mayor claridad el procedimiento y las consecuencias de la facultad de decretar la medida cautelar de bloqueo de datos concedida a una autoridad administrativa como es la Superintendencia de Industria y Comercio. Por lo anterior, mientras se aclara normativamente, existe la propuesta jurídica de que cuando se aplique la excepción de inconstitucionalidad en los supuestos que su aplicación viole el debido proceso debido a que dentro del proceso administrativo sancionatorio no se encuentra una fase que establezca el decreto de medidas cautelares. Otra medida asignada es el registro nacional de base de datos que permite cumplir funciones de policía administrativa al llevar el registro de todas las personas que tienen datos personales almacenados, cualquiera que sea su naturaleza jurídica.

Como herramientas jurídicas de autorregulación en Colombia se tienen las normas corporativas vinculantes y las políticas de tratamiento de información.

Las normas corporativas vinculantes mantienen la confianza y seguridad en el tratamiento de datos personales facilitados entre grupos empresariales que se encuentran en distintos países, esto facilita el comercio transfronterizo de datos personales y la recolección internacional sin que se desprotejan los derechos fundamentales. Le es aplicable la *lex loci contractus* en la selección del ordenamiento jurídico base que regirá el contrato corporativo.

Las políticas de tratamiento de información son un tipo de declaración unilateral de voluntad con cláusulas que fijan la finalidad, instrumentos, condiciones, encargados, responsables y tiempo por el cual se van a recolectar, almacenar y tratar datos personales o

incorporadas dentro de un contrato mayor. Es requisito para que pueda afirmarse el consentimiento informado del titular para tratar datos personales.

Existen un conjunto de datos personales que sólo se les aplica los principios administradores de datos personales del régimen general de datos personales porque entran de la finalidad establecida surge la colisión con otro derecho fundamental como la intimidad, salud, la libertad de prensa o algún principio del estado social de derecho como el de seguridad nacional o ciudadana. Por lo anterior deben regularse por leyes específicas así como sus herramientas jurídicas de protección.

Pueden presentarse una colisión de derechos fundamentales donde será necesario utilizar la ponderación como método para decidir la prevalencia en cada caso. Esto es posible aplicando las restricciones en el ámbito de aplicación del derecho fundamental que cede frente al “mayor peso” del otro derecho. Con frecuencia se presentará una colisión con los derechos a la información, la salud, la libertad de prensa, la intimidad, la vida y la seguridad ciudadana.

El nivel adecuado de protección es una noción instrumental para garantizar el cumplimiento de las normas sobre tratamiento de datos personales de cualquiera de los países que no originaron los dos modelos internacionales en aquellos a los cuales se transfiere. Es una medida de confiabilidad que de cumplirlo trae beneficios económicos a ojos de las empresas de esos países. Esencialmente revisan la regulación sustancial con derechos, obligaciones, autoridades públicas y la regulación procesal con acciones judiciales, autorregulaciones o procedimientos administrativos.

Para Colombia es vital analizar el grado de protección jurídica para atraer los nuevos sectores económicos que están surgiendo de la economía de la información. El aspecto sustancial se cumple con el nivel de protección para la norma 1266 de 2008, queda pendiente el análisis del nivel de protección en el aspecto sustancial de la ley 1581 de 2012 frente al test aplicado. De manera preliminar se encuentra la ausencia de algunos principios rectores importantes en la ley 1581 de 2012 como los de precisión en el tratamiento, límites en la recolección de información y rendición de cuentas.

Sobre todo destacar los principios de transparencia, rendición de cuentas y enfoque centrado en el usuario pues permite que se le conciba como ser humano con una dignidad inherente, impidiendo que se le tenga por simple contenedor de información, que es útil en la medida que entregue información personal para ofrecerle mejores productos, dejándolo ignorante de los procesos de tratamiento que se realizan entre el momento que recolecta la información y la entrega de los servicios y productos.

Sin embargo en el aspecto procesal se echan en ausencia las herramientas jurídicas de los códigos deontológicos, las normas corporativas vinculantes, la acción ejecutiva y el régimen específico de responsabilidad civil para el tratamiento indebido de datos personales.

Las normas corporativas vinculantes tienen una problemática fundamental respecto al reclamo de los derechos ARCO o ARCARS debido a que fundamentalmente el tema no ha sido regulado por la Autoridad de Protección de Datos Personales de Colombia, pero una razón más importante es que el titular del dato personal no es una parte en el contrato que se realiza y a pesar del reconocimiento implícito, jurídicamente no podría exigir su cumplimiento ante las autoridades de protección de datos personales por el hecho de la autorregulación inherente a este mecanismo. Sin embargo si podría alegar una responsabilidad civil extracontractual es viable por el daño comprobado ante la transferencia internacional que le perjudicó como terceros beneficiarios que vieron frustrado sus aspiraciones al pactar con el responsable del tratamiento que encabeza el grupo empresarial.

Se recomienda que la Autoridad Pública de Control sea ejercida por un ente creado especialmente para ello y no como una dependencia delegada por parte del Superintendente de Industria y Comercio pues resta capacidad decisoria y autonomía financiera.

En este punto específico se necesita que la Superintendencia de Industria y Comercio tenga una mayor capacidad financiera para promover los temas concernientes a la transparencia y rendición de cuentas, a la auditoría de la información y la definición junto con

el mercado de servicios de la información criterios autorreguladores referentes a las mejores prácticas de manejo de los datos personales en las empresas. Así éstas podrán incorporar los principios filosóficos a sus modelos de negocio, adaptando no sólo los parámetros y políticas de tratamiento de datos personales sino también la infraestructura y los sistemas de información.

En esta sociedad que utiliza la tecnología como herramienta para la vida, se busca evitar que el hombre sea convertido en un hombre unidimensional que sólo provee información y se le entregan servicios, como autómata consumidor despersonalizado, pese a que se alegue la recolección de información como necesaria para ofrecer un buen servicio.

El habeas data es un nuevo derecho que responde a las circunstancias técnicas del momento actual, en que hay tecnología que permite analizar grandes cantidades de información a un costo ínfimo, lo resalta un valor incalculable al momento de tomar decisiones o formular políticas de desarrollo empresarial o desarrollo público. A las personas se les reconoce el derecho a controlar su información personal y a que esta sea tratada conforme a unos parámetros predefinidos y formulados a partir de la experiencia que respeta otros derechos fundamentales conexos y en especial la dignidad humana.

Esta incertidumbre en las herramientas que permiten garantizar el derecho del Habeas Data incidirá profundamente en la generación de oportunidades alrededor de las tecnologías de la información, por este motivo el trabajo propone el reto de asumir un debate alrededor de su incorporación en el ordenamiento jurídico iniciando con investigaciones posteriores que aportarán los insumos suficientes para resolver el tema. Será bastante útil la teoría de la *Privacy by design* porque permite comprender como puede combinarse los parámetros técnicos con las normas legales para incluirlos en las actividades de tratamiento de datos personales.

REFERENCIAS BIBLIOGRÁFICAS

- Alemania. Tribunal Constitucional federal. Sentencia 1 BvR 209/83 del 15 de diciembre de 1983. Traducida al español por Mnauel Daranas y publicado en: N°33, Enero, 1984. *Boletín de Jurisprudencia Constitucional*, 126-170. Madrid: Congreso de los Diputados.
- Alessandri, A. (1943). *De la responsabilidad extracontractual en el derecho civil chileno*. Chile: Imprenta Universitaria.
- Alexy, Robert (1ra. Edición en 1998, 2da. Edición en 2007). *Teoría de los derechos fundamentales*. Madrid: CEPC.
- Alexy, Robert. (2000). La institucionalización de los derechos humanos en el Estado constitucional democrático. En: *Derechos y Libertades: revista del Instituto Bartolomé de las Casas*. ISSN: 1133-0937. V (8) p.21-42 (Ene-jun 2000) Universidad Carlos III de Madrid. Instituto Bartolomé de las Casas: Boletín Oficial del Estado. Recuperado el 13/02/16 de: <http://e-archivo.uc3m.es/handle/10016/1372>
- Benda, E.(2004). “Capítulo X. El Estado social de derecho”. En: Mainhoffer, Benda, Hesse, Vogel y Heyde. *Manual de derecho Constitucional*. Madrid: Tecnos.
- Benda, E.(2004). “Capítulo IV. Dignidad humana y derechos de la personalidad”. En: Mainhoffer, Benda, Hesse, Vogel y Heyde. *Manual de derecho Constitucional*. Madrid: Tecnos.
- Bobbio, N. (1993). *Igualdad y Libertad*. Barcelona: Paidós.
- Böckenfordel, E. W. (2000). “Origen y cambio del concepto de Estado de Derecho”, en Böckenfordel, Ernst Wolfgang (2000). *Estudios sobre el estado de derecho y la democracia*. 17-46 Madrid: Tecnos.
- Böckenforde, E.W.(1993). *Escritos sobre derechos fundamentales*. Baden-Baden: Nomos.
- Brian Nougrères, A. (2012). “La protección inteligente de los datos personales”. En: *Revista Internacional de Protección de Datos Personales*. ISSN: 2322-9705. N°1 Julio-Diciembre. Recuperado el 29/02/16 de: http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian-Nougreres_FINAL.pdf
- Castillo, J.L., Blanco, B y Pérez Flórez, R.(2010) La protección de la información y los datos como delito informático en Colombia: sanciones penales.
- Carrascosa González, J. (2013). *Autonomía de la voluntad. Elección de la ley aplicable al contrato internacional*. Bogotá: Universidad de la Sabana y Grupo Editorial Ibáñez.

Castro Ospina, S.(2008)*Algunos aspectos dogmáticas de la delincuencia informática*. Madrid: Portaley nuevas tecnologías. Disponible en: <http://www.delitosinformaticos.com/02/2008/noticias/algunos-aspectos-dogmaticos-de-la-delincuencia-informatica>

Cerda Silva, Alberto. (2011)El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea. *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso* [online], n.36, pp. 327-356. ISSN 0718-6851. Consultado el 30/05/2016.

Cerda Silva, A. (Diciembre, 2006). Mecanismos de Control en la Protección de Datos en Europa. *Ius et Praxis*. Revista de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, núm. 12, 221-251. Recuperado en 09 de abril de 2015, de http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122006000200009&lng=es&tlng=es. 10.4067/S0718-00122006000200009

Cerda Silva, A. (Enero, 2003). Autodeterminación informativa y leyes sobre protección de datos. *Revista Chilena de Derecho Informático*, [S.l.], n. 3, ISSN 0717-9162. Disponible en: <http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/view/10661/11413> . Fecha de acceso: 24 ene. 2016 doi:10.5354/0717-9162.2003.10661.

Chanamé Orbe, R. (2003). Habeas Data y el derecho fundamental a la intimidad de la person. Maestria. Universidad Nacional Mayor de San Marcos: Lima.

Colombia. Corte Constitucional. Sentencia C-748 de 2011 del 6 de octubre de 2011. Magistrado Ponente Jorge Ignacio Pretelt Chaljub.

Colombia. Corte Constitucional. Sentencia T-814 de 17 de septiembre de 2003. Magistrado Ponente Rodrigo Escobar Gil. Consultada el día 04/05/16 en: <http://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm>

Colombia. Corte Constitucional. Sentencia T-729 de 2002. Magistrado Ponente Eduardo Montealegre Lynett. Consultada el día 04/05/16 en: <http://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm>

Colombia. Corte Constitucional. Sentencia SU-082 de 1 de marzo de 1995. Magistrado Ponente Jorge Arango Mejía. Consultada el día 04/05/16 en: <http://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm>

Colombia. Corte Constitucional. Sentencia T-414 de 1992 del 16 de junio de 1992. Magistrado Ponente Ciro Angarita Barón. Consultada el día 04/05/16 en: <http://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm>

Colombia. Corte Constitucional. Sentencia T-512 de 1992 del 09 de septiembre de 1992. Magistrado Ponente José Gregorio Hernández Galindo.

- Colombia. Congreso de la República. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 1993. no.47223. Recuperado el 23 de Enero de 2016 en: http://www.secretariassenado.gov.co/senado/basedoc/ley_1273_2009.html
- Colombia. Congreso de la República. Ley Estatutaria 1581 (17, Octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá: Diario Oficial No. 48.587 de Octubre 18 de 2012. Recuperado el 23 de Enero de 2016 en: http://www.secretariassenado.gov.co/senado/basedoc/ley_1581_2012.html
- Colombia. Ministerio de Industria y Comercio. Decreto 1377. (27, junio, 2013). Por el cual se reglamenta parcialmente la ley 1581 de 2012. Recuperado en 26 de marzo de 2015 de, www.mincit.gov.co/descargar.php?id=68585.
- Colombia. Ministerio de Industria y Comercio. Decreto 886. (13, mayo, 2014). Por el cual se reglamenta el artículo 25 de la ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos. Diario Oficial. Bogotá, D.C., 1993. no.41148. p.1-168. Recuperado en 09 de abril de 2015 de, <http://wsp.presidencia.gov.co/Normativa/Decretos/2014/Documents/MAYO/13/DECRETO%20886%20DEL%2013%20DE%20MAYO%20DE%202014.pdf>
- Colombia. Presidencia de la República. Decreto 25 de 2014 (10, de Enero, 2014,).Por el cual se modifica la estructura orgánica y se establece la organización y funcionamiento de la Defensoría del Pueblo. Diario Oficial, Bogotá no. 49.209. Recuperado el 06/06/2016 de: http://www.secretariassenado.gov.co/senado/basedoc/decreto_0025_2014.html
- Cortés Rodas, F. (2011). *El contrato social liberal: John Locke. Co-herencia*, Vol.7 núm.13, pp. 99-132. Recuperado el día 13/03/2016 de: <http://publicaciones.eafit.edu.co/index.php/co-herencia/article/view/33>
- De Cupis, Adriano. *El Daño. Teoría General de la Responsabilidad Civil*.
- Del Vecchio G. (1971). *Los principios Generales del Derecho*. Barcelona: Bosch.
- Douzinas, Costas (2008). *El fin de los derechos humanos*. Bogotá: Legis S.A.
- España. Tribunal Constitucional. Sentencia 254 del 20 de julio de 1993. Recurso de amparo N°1827 de 1990.Consultado el 20 de Mayo de 2016 en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/tribunal_constitucional/common/pdfs/13_Sentencia_254-1993_de_20_julio_1993_def_-_copia.pdf
- García Castillo, T. (2010). La lex contractus en los contratos internacionales. En: Méndez-Silva, R. (Coord.). *Contratación y arbitraje internacional*. México: Instituto de Investigaciones Jurídicas de la Universidad Autónoma de México. Recuperado el 07/06/2016 de: <http://biblio.juridicas.unam.mx/libros/libro.htm?l=2776>

- Giraldo Angel, Jaime (2007). Metodología y técnica de la investigación jurídica. Bogotá: Librería Ediciones del Profesional.
- González Rus, Juan José. (2004) Protección penal de sistemas, elementos, datos, documentos y programas informáticos. Revista Electrónica de Ciencia Penal y Criminología RECPC, N°1 (en línea). Universidad de Granada, España. Disponible en:http://criminet.ugr.es/recpc/recpc_01-14.html.
- Henao, Juan Carlos. (1998). *El Daño. Análisis comparativo de la responsabilidad extracontractual del Estado en derecho colombiano y francés*. Bogotá: Universidad Externado de Colombia.
- Heller, Hermann (1942, Reimp.2007). *Teoría del Estado*. México: Fondo de Cultura Economía –FCE.
- Julio Estrada, A.(2000). *La eficacia de los derechos fundamentales entre particulares*. Bogotá: Universidad Externado de Colombia.
- Kant,I.(1797, trad.1873) *Metaphysische Anfangsgründe der Rechtslehre*, Königsberg. Traducción al castellano de G. Lizarraga: *Principios metafísicos del derecho*, Madrid.
- Locke, John (1991, 2006). *Segundo Tratado del Gobierno Civil*. Madrid: Tecnos
- Mantilla Espinosa, Fabricio. (2007). El principio general de responsabilidad por culpa del derecho privado colombiano. *Revista Opinión Jurídica*, 6(11), 131-150. Recuperado 02/03/16 de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1692-25302007000100008&lng=en&tlng=es.
- Ojeda-Pérez, Jorge Eliécer, Rincón-Rodríguez, Fernando, Arias-Flórez, Miguel Eugenio, & Daza-Martínez, Libardo Alberto. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad*, 11(28), 41-66. Retrieved June 05, 2016, from http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=en&tlng=es.
- Organización de las Naciones Unidas. (Resolución 45/95 de 4 de diciembre de 1990) *Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales*. Recuperado el 28 de abril de 2016 en <http://inicio.ifai.org.mx/Estudios/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf>
- Osuna Patiño, Néstor Iván (1998). Tutela y amparo: derechos protegidos. Bogotá: Universidad Externado de Colombia.

- Paez, A. y Vera, J. (2015) Sanciones por parte de la Superintendencia de Industria y Comercio por el cambio de la finalidad en el uso de los datos personales en Colombia período 2013-2014. Universidad Libre, Seccional Cúcuta
- Peces-Barba Martínez, G. (1986). Sobre el puesto de la historia en el concepto de los derechos humanos. *Anuario de Derechos Humanos*, N°4, 219-258. Recuperado el 12/02/16 de: <http://e-archivo.uc3m.es/handle/10016/10383>
- Peces-Barba Martínez, G. (1988) Sobre el fundamento de los derechos humanos: un problema de moral y Derecho. *Anales de la Cátedra Francisco Suárez*, N°28, 193-207. Recuperado el 09/02/2016 en: <http://e-archivo.uc3m.es/handle/10016/11490>.
- Peces-Barba, G. (2007) De la miseria del hombre a la dignidad humana. En: *Anales de la Real Academia de Ciencias Morales y Políticas*, 2007, n. 84, p. 167-180. Consultado el 30/05/16: <http://e-archivo.uc3m.es/handle/10016/11803#preview>
- Perez Escobar, Jacobo (2013). Metodología y técnica de la investigación jurídica. Bogotá: Temis.
- Perez Luño, A. (1988) *Los derechos fundamentales*. Madrid: Tecnos.
- Pérez Luño, A. (2005) *Derechos humanos, estado de derecho y constitución*. Madrid: Tecnos.
- Pérez Luño, A. (2006) *La tercera generación de derechos humanos*. Navarra: Aranzadi.
- Pérez Salazar, Gonzalo (2013) “Naturaleza Jurídica del Habeas Data”, en Velandia Canosa, Eduardo Andrés (Dir. Cient.), Derecho Procesal Constitucional, Vol. IV, pp. 681-710. Bogotá: VC Editores y ACDPC.
- Piñar Mañas, J. (2011). El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. *Cuadernos De Derecho Público*, (19-20). Recuperado de <http://revistasonline.inap.es/index.php?journal=CDP&page=article&op=view&path%5B%5D=692&path%5B%5D=747>
- Posada Maya, R. (Agosto, 2006). Aproximación a la criminalidad informática en Colombia. En: *Revista de derecho, comunicaciones y nuevas tecnologías*, núm.2, pp.13-60, Facultad de Derecho de la Universidad de los Andes. Colombia. Recuperado el 04/06/16 de: https://derechoytics.uniandes.edu.co/components/com_revista/archivos/derechoytics/ytics86.pdf
- Pressman, Roger (2010). Ingeniería del software, un enfoque práctico. México: McGraw-Hill.
- Prosser, W. (Agosto, 1960). Privacy. *California Law Review*, Volumen 48, Núm.3. 383-423. Recuperado el 17/02/16 de: <http://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1>

- Puccinelli, O. (2004) Evolución histórica, análisis de las diversas especies, subespecies, tipos y subtipos de habeas data. *Vniversitas*, núm. 107, pp. 471-501, Pontificia Universidad Javeriana. Colombia.
- Remolina-Angarita, N. (2013) *Tratamiento de datos personales. Aproximación internacional y comentarios a la ley 1581 de 2012*. Bogotá: Legis.
- Remolina-Angarita, N.(2012). Aproximación constitucional de la protección de datos personales en Latinoamérica. En: *Revista Internacional de Protección de Datos Personales*. ISSN: 2322-9705. N°1 Julio-Diciembre. Recuperado el 02/03/16 de: http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf
- Remolina-Angarita, N. (Enero-Junio, 2010a). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *International Law*, N°16.489-524. Recuperado el 19 de abril de 2016 de: <<http://www.redalyc.org/articulo.oa?id=82420041015>>
- Remolina-Angarita, N. (2010b) Cláusulas contractuales y transferencia internacional de datos personales, en Oviedo Albán, Javier (Coord.), *Obligaciones y contratos en el derecho contemporáneo*. Bogotá: Diké-Universidad de la Sabana.
- Remolina-Angarita, N. (Noviembre, 1994). El habeas data en Colombia. *Revista de Derecho Privado*, núm.15. Facultad de Derecho de la Universidad de los Andes. Recuperado en 09 de abril de 2015, de https://derechoprivado.uniandes.edu.co/components/com_revista/archivos/derechoprivado/pri319.pdf
- Rey Cantor, E. & Rodriguez Ruíz, M. (2005) *Las generaciones de los derechos humanos. Libertad-Igualdad-Fraternidad*. Bogotá: Universidad Libre.
- Saarenpää, A. (Diciembre, 2003). Europa y la protección de los datos personales. *Revista de Derecho Informático*. N°3.pp 15-29. Consultado el 05/06/2015 en: http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_complex/0,1491,SCID%253D14232%2526ISID%253D507,00.html
- Solove, Daniel J., Taxonomy of Privacy”(2006) *University of Pennsylvania Law Review*, Vol. 154, No. 3, p. 477-560, January . Consultado el 02/04/2014: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622 o en [https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.R.ev.477\(2006\).pdf](https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.R.ev.477(2006).pdf)
- Sierra Porto, Humberto (1998).*Concepto y tipos de ley en la constitución colombiana*. Bogotá: Universidad Externado de Colombia.
- Suárez Espino, M. (2008). El derecho a la intimidad genética. Madrid: Marcial Pons.

Tamayo Jaramillo, Javier (2007). *Tratado de Responsabilidad Civil*. Bogotá: Legis

Unión Europea. Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales (CE, 2007), *Dictamen 4/2007 sobre el concepto de datos personales*. Bruselas. Consultado el 29/04/16 de: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf

Unión Europea. Parlamento europeo y Consejo europeo. (24 de octubre de 1995) Directiva 95/46/CE “relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos”. Recuperado el 5 de julio de 2015 de, http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_es.pdf

Unión Europea. Comisión Europea. (26 de junio de 1997) Documento de trabajo N° WP4 “*Primeras orientaciones sobre la transferencia de datos personales a países terceros Posibles formas de evaluar la adecuación*”. Recuperado el 8 de junio de 2016 de, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_es.pdf

Unión Europea. Comisión Europea. (24 de julio de 1998) Documento de trabajo N° WP12 “*Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE*”. Recuperado el 8 de junio de http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_es.pdf

Unión Europea. Comisión Europea, Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales ((16 de febrero de 2010)), *Dictamen 1/2010 sobre los conceptos responsable del tratamiento y encargado del tratamientos*. Bruselas. Consultado el 12/05/16 de: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf

Unión Europea. Parlamento europeo y Consejo Europeo (27 de abril de 2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Recuperado el 24/05/16 de: <http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES>

Valencia Zea, A. & Ortiz Monsalve, A. (2006) Derecho civil. Tomo 1, parte general y personas. Bogotá: Temis

Warren, Samuel & Brandeis, Louis. (Diciembre, 1890). The Right to Privacy. *Harvard Law Revie*. The Harvard Law Review Association, Volumen 4, núm.5, 193-220. Recuperado el 20 de abril de 2015 de: <http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf>

Zabala, Matilde (1982). Derecho a la intimidad. Buenos Aires: Abeledo-Perrot.

ANEXOS

Anexo A

GUIA DE ANALISIS DOCUMENTAL	
OBSERVADOR :	GUIA N° _____ de ___/___/20___
Propósito del diligenciamiento: Obtener la información pertinente sobre la posición jurisprudencial en la aplicación de la ley estatutaria de protección de datos personales y sus mecanismos. De esta manera se va a identificar y comprender la línea jurisprudencial de los jueces.	
Referencia Bibliográfica	
Tema	
Conceptos Clave	
Idea principal	
Ideas secundarias relevantes	
Análisis conceptual del documento	
Aportes del texto	
Polémicas	
Preguntas que suscita el texto	
Comentario Personal	
Referencia de otros autores	

FIRMA

Anexo B

GUIA DE ANALISIS JURISPRUDENCIAL	
OBSERVADOR :	GUIA N° _____ de ___/___/20___
Propósito del diligenciamiento: Obtener la información pertinente sobre la posición jurisprudencial en la aplicación de la ley estatutaria de protección de datos personales y sus mecanismos. De esta manera se va a identificar y comprender la línea jurisprudencial de los jueces.	
Identificación de la Providencia	
Corporación y Sala Sentencia N° Medio de Acción Fecha Magistrado Ponente	

1. Posición jurídica de la parte actora

- d) Hechos Relevantes:
- e) Argumentos Jurídicos del Accionante
- f) Pretensiones.

2. Posición jurídica del demandado

- c) Excepciones aducidas por la Entidad Demandada
- d) Argumentos jurídicos del Demandado

3. Planteamiento del problema jurídico

4. Fallo de Instancia

- d) Consideraciones
- e) Decisión de Primera Instancia

5. De la Segunda Instancia

- f) Consideraciones respecto al problema jurídico
- g) Tesis de la Corporación
- h) Fundamentos de la Tesis de la Corporación
- i) Salvamentos de voto

6. Análisis Crítico

- h) Identificación de precedentes
- i) Reglas aplicadas
- j) Comentario

FIRMA

ANEXO C

GUIA DE ANALISIS NORMATIVO	
Autor del análisis :	GUIA N° _____ de ____/____/20____
Propósito del diligenciamiento: Realizar el análisis sistemático y teleológico de las normas sobre protección de Habeas Data que se encuentran vigentes en el ordenamiento colombiano y en convenciones, acuerdos o tratados vinculantes e influyentes.	
Ley [] Por la cual (...)	
Artículo	Análisis
	Preguntas que suscita
Artículo	Análisis
	Preguntas que suscita

NOTA: Se agregan tantas filas como sea necesario

FIRMA