La protección general de datos personales, su relación con el derecho a la libertad de información y los efectos que en este produce.

Monografía Jurídica para optar por el título de Abogado

Nicolás David Escobar Ortiz

Asesor

Sebastián Arboleda Cardona

Abogado

Corporación Universitaria Lasallista
Facultad de Ciencias Sociales y Educación
Derecho
Caldas, Antioquia
2018

Tabla de contenido

Resumen

Protección de datos personales, breve aproximación a su protección, leyes relevantes y sentencias regulatorias, protección especial y protección general con base en las exigencias internacionales. Acercamiento a la creación del registro nacional de base de datos en cabeza de la Superintendencia de Industria y comercio, plasmado en la ley 1581 de 2012. Análisis de su necesidad en una sociedad donde la tecnología hace parte de la cotidianidad.

Palabras clave:

Información, Derecho a la información, Dato, Datos personales, Registro nacional de base de datos.

Introducción

Desde el inicio de los tiempos el ser humano se ha preocupado por mantener el control sobre la información que en el medio se maneja de él. Es este control el que ha generado la necesidad a través de la historia de crear normativas que permitan proteger y regular su información. Nace así la división entre información pública e información privada. División que permite que cierta información pueda ser conocida por toda la sociedad (siempre que el sujeto así lo permita, o que se trate de manifestaciones realizadas en espacios públicos) y que otro tipo de información sea manejado solamente en un contexto de reserva (privacidad) la cual estará en control del titular de esta información y de las personas a las cuales el titular expresamente les otorgue esta información. En este trabajo se tratará de hacer un recorrido por la historia de la protección a la información en especial los datos personales, las creaciones normativas más relevantes y las que se encuentran vigentes hoy en día, las sentencias que han regulado este tema y la entidad encargada de velar por la protección de los datos personales.

Justificación

La importancia de este trabajo está en el beneficio que generará para la academia una breve profundización, conocer y evidenciar como el Estado Colombiano está enfocando la protección de los derechos fundamentales, en este caso frente al derecho a la información específicamente, la protección que sea realiza a los datos personales. Este trabajo además de brindar al receptor del mensaje la opción de crearse una posición frente a la protección de estos derechos, permitirá conocer cuál ha sido la creación normativa por parte del estado para regulación de estos derechos, además de las principales entidades encargadas de su protección.

Objetivos

General:

Explorar el efecto que la reciente ley de protección de datos personales tiene sobre el derecho de libertad de información, como su aplicación genera una violación al derecho a la libertad de información.

Específicos:

Desarrollar un marco normativo, jurisprudencial y teórico sobre el derecho a la libertad de información en Colombia.

Comparar la normativa internacional sobre protección de datos personales con la Ley 1581 de 2012, y sus decretos reglamentarios.

Estudiar e identificar casos emblemáticos en la jurisprudencia colombiana de ponderación entre la libertad de información y la protección de datos personales, permitiendo la visualización de la línea jurisprudencial adoptada por las altas cortes frente a este tema.

Marco teórico

“Dadme la libertad de saber, de hablar y de argüir libremente según mi conciencia, por encima de todas las libertades” (Milton, Jhon. Areopagítica 2000 versión)

A través de la historia, el deseo del ser humano por el conocimiento ha sido una constante, la necesidad por tener nuevos saberes fue uno de los factores que ha permitido que la civilización haya avanzado hasta lo que hoy conocemos. Generalmente quien controla la información, controla el resultado de las cosas. Desde decidir el curso de una batalla, de una guerra, hasta el desarrollo político de un país. Como mencionó el filósofo chino Sun Tzu y que en su libro el arte de la guerra menciona lo siguiente**:**

> Así, sólo un gobernante brillante o un general sabio que pueda utilizar a los más inteligentes para el espionaje, puede estar seguro de la victoria. El espionaje es esencial para las operaciones militares, y los ejércitos dependen de él para llevar a cabo sus acciones***.***

Para este filósofo era claro la gran importancia que tenía el manejo de la información, importante para tomar las decisiones antes de ir a la batalla. Esta necesidad de controlar la información, para tener la ventaja y poder tomar decisiones teniendo en cuenta el conocimiento previo ha existido y seguirá existiendo, los reyes, la iglesia, ha procurado por realizar un control sobre la información, ya sea indicando mediante leyes que, su pensamiento puede ser el único verdadero y de esta forma censurando los pensamientos de los demás que estos sujetos consideren no son acordes a sus ideales, de esta forma se estaba realizando un control sobre la información en otras palabras se realizaba una censura sobre esta información, sin importar si esta se trataba de una información real o ficticia. En estas épocas, la búsqueda de la información por parte de las personas del común suponía un peligro, ya que, si esta búsqueda iba en contra de

la información que los altos poderes hacían circular, ponía en juego la propiedad privada del sujeto, su libertad y hasta su vida. Muchos casos de estas personas que buscaron el conocimiento y este era diferente del planteado por los dueños del poder, eran considerados como herejes, brujos que debían morir por contrariar las enseñanzas de Dios. Está fue una época oscura para la búsqueda del conocimiento, que género que se crearan grupos clandestinos para la búsqueda e intercambio de la información. Este control, al no diferenciar el tipo de información que acumulaba o en algunos casos el fin era tomar toda la información posible de los sujetos los cuales se estaban investigando ya fueran propios o extranjeros, empezó a generar cierto malestar entre las personas, al evidenciar que este tipo de práctica no tenía regulación y permitía que cualquiera que tuviera la posibilidad, tomara la información de otra persona, sin importar de qué tipo de información se tratara. De este hecho nace la necesidad de regular la información, la necesidad de proteger los datos que están en el medio y que estaban siendo captados por cualquier tipo de persona, se crea la obligación de proteger la información cuando se trata de temas netamente privados los cuales solo son importantes para la persona de la cual nacen los datos, esta necesidad de proteger la información, de que lo que una persona no quiera que salga al público, no lo haga. Pero proteger la información, ya sea pública o privada no es una tarea fácil. La falta de regulación por parte del Estado frente a este tema y la necesidad y deseo de la sociedad de ir cada día más hacia una sociedad donde la información que recibe el receptor no presenta ninguna modificación y se presenta tal cual lo acontecido, hace que se busque cada vez más que la información no se contamine por posiciones de los sujetos que la recaudan y la suministran, a su vez las redes sociales con su alta posibilidad de poner en contacto a la mayoría de las personas en cuestión de segundos genera que el flujo de información que se almacena

en estas plataformas virtuales siempre este en un peligro constante de ser vulnerada y caer en manos de personas que pueden compartirla con el resto del mundo o de extorsionar a la persona de la cual tomaron la información, usurpar su identidad y realizar actividades ilícitas con esta.

Es en Francia con la expedición de la declaración de los derechos del hombre y del ciudadano que se empieza a evidenciar la importancia que representa para el hombre tener el control sobre la información que recibe diariamente, y como este control es necesario para desarrollar la sociedad y el proyecto de vida de cada miembro de esta. En los siguientes artículos de la declaración de los derechos del hombre y del ciudadano, 1789:

> Artículo 10− Nadie debe ser incomodado por sus opiniones, inclusive religiosas, siempre y cuando su manifestación no perturbe el orden público establecido por la Ley. –
>
> Artículo 11. La libre comunicación de pensamientos y opiniones es uno de los derechos más valiosos del Hombre; por consiguiente, cualquier Ciudadano puede hablar, escribir e imprimir libremente, siempre y cuando responda del abuso de esta libertad en los casos determinados por la Ley.

La declaración de los derechos del hombre y del ciudadano emitida por el pueblo francés fue el punto de partida para que los gobiernos del mundo iniciaran una lucha por los derechos que consideraban no podían faltar dentro de cada sociedad. Se puede decir entonces que este fue una de las primeras manifestaciones protectoras del derecho a la información que fue plasmada en un documento que fue reconocido por todo un pueblo.

Nuestro país, con base en estos fundamentos históricos en su necesidad de proteger estos derechos, plasma en la Constitución Política de 1991, en los siguientes

artículos buscando la protección del derecho a la información, también conocido como derecho de prensa:

> Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.
>
> Artículo 74. Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley.
>
> El secreto profesional es inviolable.

Con la protección consagrada en el artículo 20 de la Constitución Política, se buscaba garantizar que los ciudadanos estuvieran informados de lo que hacia la administración pública del estado. Derecho que puede ser ejercido en su totalidad siempre y cuando no existiera una norma que impidiera acceder a esta información. Ya que, de este acceso a la información, el ciudadano de un estado, en este caso el colombiano, al tener en cuenta esta información, puede decidir si desea participar en el curso social de su país toda vez que así puede conocer las decisiones que ha tomado su nación y saber hacía donde quiere dirigirse. Derecho a la información que consiste tanto en el hecho de ser informado como en el de informar, con su protección se busca garantizar la protección de la trasparencia del Estado Colombiano, al permitir que la mayoría de su información pueda ser vigilada permite que los ciudadanos puedan tomar decisiones basadas en el amplio conocimiento de lo que está sucediendo con su país. Se conoce de manera especial como libertad de prensa, que la Corte Constitucional definió en la sentencia T- 609 de 1992 de la siguiente manera:

> La libertad de prensa como es conocida de modo especial, consiste en el derecho fundamental para publicar y difundir las ideas por cualquier medio gráfico y es una de las características de todo régimen democrático puesto que propicia el pluralismo político e ideológico; su finalidad más trascendental es la de permitir que exista un espacio propicio para controlar los actos de los gobernantes y para indicar derroteros a los asociados, todo lo cual en principio le da a ella en el cuadro de regulaciones constitucionales una posición preferente ante los poderes públicos y ante otros derechos fundamentales autodisponibles.

Esta libertad de información debe tener en cuenta la afectación que causa con su ejercicio en los otros derechos fundamentales, que como está ligada a la libertad de prensa, cuando se expide cierta información se debe verificar que está no atente con la intimidad de una persona cuando por ejemplo la información que se expide no esté ajustada a la realidad y lo que se informó no sea totalmente, cierto como ha pasado en reiteradas ocasiones, en general con el auge de las redes sociales la desinformación se ha hecho presente cada día.

Como una muestra de la protección que el Estado colombiano realiza sobre el derecho a la información, se creó la Ley 1341 del 2009, que, aunque directamente no regulaba el derecho fundamental a la información, si permite observar la visión que tiene el Estado frente a la necesidad de proteger y regular la información en nuestro país, se puede visualizar esta idea mejor al identificar su objetivo el cual es el siguiente:

> ARTÍCULO 1o. OBJETO. La presente ley determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento

> general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información.
>
> PARÁGRAFO. El servicio de televisión y el servicio postal continuarán rigiéndose por las normas especiales pertinentes, con las excepciones específicas que contenga la presente ley.
>
> Sin perjuicio de la aplicación de los principios generales del derecho.

Esa ley fue expedida para regular de manera general las TIC (tecnologías de la información y las telecomunicaciones). Y aunque no fue expedida para regular el derecho a la información, se consagro en sus principios orientadores lo siguiente en el numeral 7 del artículo 2:

> 7. El derecho a la comunicación, la información y la educación y los servicios básicos de las TIC. En desarrollo de los artículos 20 y 67 de la Constitución Nacional el Estado propiciará a todo colombiano el derecho al acceso a las tecnologías de la información y las comunicaciones básicas, que permitan el ejercicio pleno de los siguientes derechos: La libertad de expresión y de difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, la educación y el acceso

> al conocimiento, a la ciencia, a la técnica, y a los demás bienes y valores de la cultura. Adicionalmente el Estado establecerá programas para que la población de los estratos <sic> desarrollará programas para que la población de los estratos menos favorecidos y la población rural tengan acceso y uso a las plataformas de comunicación, en especial de Internet y contenidos informáticos y de educación integral.

Garantizando de esta forma que el uso de las TIC no desconociera los derechos fundamentales que sustentan nuestro país, en este caso específico, el derecho a la información. Dentro de sus principios también se tiene en cuenta la amplia relación que juegan los datos personales (habeas data) y que fue desarrollado en el numeral número 4 del artículo 2 de la presente ley indicando lo siguiente:

> 4. Protección de los derechos de los usuarios. El Estado velará por la adecuada protección de los derechos de los usuarios de las Tecnologías de la Información y de las Comunicaciones, así como por el cumplimiento de los derechos y deberes derivados del Hábeas Data, asociados a la prestación del servicio. Para tal efecto, los proveedores y/u operadores directos deberán prestar sus servicios a precios de mercado y utilidad razonable, en los niveles de calidad establecidos en los títulos habilitantes o, en su defecto, dentro de los rangos que certifiquen las entidades competentes e idóneas en la materia y con información clara, transparente, necesaria, veraz y anterior, simultánea y de todas maneras oportuna para que los usuarios tomen sus decisiones.

Aunque no se desarrolló a fondo el tema de la protección de los derechos de los ciudadanos frente a su información, si se evidenció la importancia que este tema juega para el estado y como al hacer uso de las TIC, su protección debe aumentar.

Directamente y buscando la protección de este derecho a la información y teniendo en cuenta el auge tecnológico del país, además del hecho del uso de las TIC, el gobierno nacional expide la ley 1273 de 2009, la cual modificó el código penal estipulando lo siguiente:

> 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.

Esta modificación se da teniendo en cuenta la situación histórica y social del país, en el cual la entrada de los elementos computacionales estaba – y aun lo está- en un gran nivel de crecimiento diario, cambiando paso a paso, las formas como las personas acceden a la información. Como una forma de protección al derecho a la información se expidió la ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Esta ley tiene como objetivo lo siguiente “Artículo 1°. Objeto. El objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información**.”**

Esta ley busca garantizar el derecho a la información que es generada por las entidades obligadas, plasmándose de esta forma, en el artículo 2 de la ley lo siguiente:

> Artículo 2°. Principio de máxima publicidad para titular universal. Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley.

Con este principio se garantiza el acceso de las personas a la información en posesión de los sujetos obligados, que como ya se había indicado anteriormente, permite realizar un control a las acciones de estas entidades, además del hecho de permitir la toma de decisiones desde una situación de conocimiento, que sin el acceso a esta información no se podría lograr.

En el artículo 4 de dicha ley, el Estado plasma una limitación a este acceso a la información, cuando menciona que si una persona evidencia que esta información puede poner en riesgo tanto su integridad como la de su familia podrá solicitar realizar una limitación a este acceso a la información, esto quedó definido de la siguiente manera:

> ARTÍCULO 4o. CONCEPTO DEL DERECHO. En ejercicio del derecho fundamental de acceso a la información, toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente. Las excepciones serán limitadas y proporcionales, deberán estar contempladas en la ley o en la Constitución y ser acordes con los principios de una sociedad democrática. El derecho de acceso a la información genera la obligación correlativa de divulgar proactivamente la información pública y responder de buena fe, de manera adecuada, veraz, oportuna y accesible a las solicitudes de

> acceso, lo que a su vez conlleva la obligación de producir o capturar la información pública. Para cumplir lo anterior los sujetos obligados deberán implementar procedimientos archivísticos que garanticen la disponibilidad en el tiempo de documentos electrónicos auténticos.
>
> PARÁGRAFO. Cuando el usuario considere que la solicitud de la información pone en riesgo su integridad o la de su familia, podrá solicitar ante el Ministerio Público el procedimiento especial de solicitud con identificación reservada.

De esta forma se está garantizando que el uso que se le da a la información no vaya en detrimento de los demás derechos fundamentales. En esta misma ley se plasma una definición de lo que se entiende por el Estado colombiano sobre información, en su artículo 6 la cual fue definida así:

> ARTÍCULO 6o. DEFINICIONES.
>
> a) Información. Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen;
>
> b) Información pública. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal;
>
> c) Información pública clasificada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley;

d) Información pública reservada. Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley;

e) Publicar o divulgar. Significa poner a disposición en una forma de acceso general a los miembros del público e incluye la impresión, emisión y las formas electrónicas de difusión;

f) Sujetos obligados. Se refiere a cualquier persona natural o jurídica, pública o privada incluida en el artículo 5o de esta ley;

g) Gestión documental. Es el conjunto de actividades administrativas y técnicas tendientes a la planificación, procesamiento, manejo y organización de la documentación producida y recibida por los sujetos obligados, desde su origen hasta su destino final, con el objeto de facilitar su utilización y conservación;

h) Documento de archivo. Es el registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones;

i) Archivo. Es el conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia. También se puede entender como la institución que está al

> servicio de la gestión administrativa, la información, la investigación y la cultura;
>
> j) Datos Abiertos. Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos;
>
> k) Documento en construcción. <Literal CONDICIONALMENTE exequible> No será considerada información pública aquella información preliminar y no definitiva, propia del proceso deliberatorio de un sujeto obligado en su calidad de tal.

En estas definiciones se plasmaron las formas más claras en las que se puede encontrar la información, y se define información como un conjunto de datos.

Mediante la sentencia C 274 de 2013 expedida por la Corte Constitucional, se realizó el control de constitucionalidad de la ley 1712 de 2014, la Corte Constitucional también estableció la línea jurisprudencial mediante la cual había tratado la clasificación de la información la cual definió dela siguiente forma:

> De conformidad con los parámetros constitucionales señalados en la jurisprudencia, la Corte ha consagrado las siguientes reglas: (i) Cuando se trate de un dato personal sensible, en principio, sólo su titular podría tener acceso. Sobre el particular, la Corte puntualizó lo siguiente en la sentencia C-1011 de 2008: “Caso distinto se predica de la información sensible,

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

En este caso, 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. (ii) A partir de la clasificación de la información en personal o impersonal y en pública, privada, semiprivada o reservada, la Corte resumió en los siguientes términos las reglas para determinar si tal información se encuentra sujeta a reserva o si por el contrario puede ser revelada, en la sentencia T-161 de 2011: 13.- A partir de esta clasificación es posible determinar si la información se encuentra sujeta a reserva o si por el contrario puede ser revelada, de modo que: - La información personal reservada contenida en documentos públicos: No puede ser revelada. - Los documentos públicos que contengan

información personal privada y semi-privada: El ejercicio del derecho al acceso a documentos públicos se despliega de manera indirecta, a través de autoridades administrativas o judiciales (según el caso) y dentro de los procedimientos (administrativos o judiciales) respectivos. - Documentos públicos que contengan información personal pública: Es objeto de libre acceso. 14.- En relación con la reserva esta Corporación ha establecido que esta puede versar sobre el contenido de un documento público pero no respecto de su existencia, así se estableció que “el secreto de un documento público no puede llevarse al extremo de mantener bajo secreto su existencia. El objeto de protección constitucional es exclusivamente el contenido del documento. Su existencia, por el contrario, ha de ser pública, a fin de garantizar que los ciudadanos tengan una oportunidad mínima a fin de poder ejercer, de alguna manera, el derecho fundamental al control del poder público (art. 40 de la C. P.)” Adicionalmente esta Corporación señaló que la: “reserva puede ser oponible a los ciudadanos pero no puede convertirse en una barrera para impedir el control intra o interorgánico, jurídico y político, de las decisiones y actuaciones públicas de que da cuenta la información reservada.” Y seguidamente expresó “La reserva legal sólo puede operar sobre la información que compromete derechos fundamentales o bienes de relevancia constitucional pero no sobre todo el proceso público dentro del cual dicha información se inserta.” Se concluye entonces que es necesario que las autoridades estatales permitan el acceso a la información que permita por parte de los ciudadanos el control de las decisiones tomadas por dichos órganos. (iii) Con el fin de determinar

la intensidad con que una información personal se encuentra ligada la esfera íntima del individuo, a partir de la clasificación precitada, la Corte, en la sentencia C-692 de 2003, señaló: De la tipología que acaba de citarse es posible inferir que aunque cierto tipo de información permanece confinada al ámbito personalísimo del individuo, otro tipo, que también le concierne, puede ser conocida por el Estado mediante orden de autoridad judicial competente o por disposición de las entidades administrativas encargadas de manejarla. De lo anterior también se deduce que cierta información que concierne al individuo puede ser divulgada sin el cumplimiento de requisitos especiales, al tiempo que otros datos, contentivos de información ligada a su ámbito personal, requieren autorización de autoridad competente o simplemente no pueden ser divulgados. Así entonces, corresponde a las autoridades administrativas o judiciales determinar, en los casos concretos sometidos a su consideración, a qué tipo de información corresponden los datos por ellas solicitados o administrados, a fin de establecer si por solicitarlos o administrarlos se incurre en intromisión indebida en el ámbito íntimo del individuo. Lo anterior debe entenderse acompasado por el cumplimiento de las normas que, sobre administración de datos personales, ha sistematizado la jurisprudencia constitucional. En este sentido, además de determinar el tipo de información que puede ser divulgada y el que no puede serlo, las autoridades administrativas y judiciales están en la obligación de guiarse por los principios de libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida,

> caducidad e individualidad del dato, con el fin de garantizar la protección, no sólo del derecho a la intimidad, sino también la del habeas data.

Además, la Corte Constitucional índica la obligación que se debía tener presente a la hora de realizar una difusión de la información, indicando lo siguiente:

> El derecho a acceder a la información pública incluye también el derecho a difundirla responsablemente, y a la luz de lo que ha señalado esta Corporación, implica que la difusión de la información debe hacerse respetando fielmente su contenido, el contexto en el cual él se produjo y sin el propósito de crear confusión o desorientación. Pero tal uso responsable no implica la obligación de corroborar la veracidad de una información que se presume debe ser cierta. Debido al papel que cumple el acceso a la información pública como instrumento para el control del poder público, el manejo de los recursos públicos y para el fortalecimiento de la democracia, la veracidad de la información que entrega el sujeto obligado a quien la solicita es esencial para el cumplimiento de esos fines constitucionales. Por ello el artículo 3 enfatiza la importancia de los principios de buena fe, transparencia, facilitación y de calidad de la información, como elementos esenciales para la protección de este derecho. Aun cuando se da por supuesto que la información pública debe ser cierta y veraz, la expresión “atendiendo a la veracidad de la misma”, introduce la idea de que es posible que una autoridad pública entregue información que no sea verídica a quien la solicita y que en esa circunstancia se traslade la responsabilidad al que la use o difunde, pero no la concentre en el que la emite, lo cual genera ciertamente una carga

> manifiestamente desproporcionada para la persona que accede a la información. Adicionalmente, establecer responsabilidad por el uso de la información en esas circunstancias, conduciría a que el ciudadano que decida difundir dicha información pública, tenga que abstenerse de hacerlo hasta tanto no compruebe que la que le ha sido suministrada es cierta, lo cual constituye un obstáculo irrazonable y desproporcionado para el ejercicio de este derecho, para el cumplimiento de las funciones de control a la actividad estatal que lo justifican y para el desarrollo del principio de participación democrática. Aceptar que la difusión de información pública depende de su veracidad, podría acarrear además responsabilidades civiles y hasta penales para quien la difunda, con lo cual se impondría una carga desproporcionada a los usuarios. En esa medida, la expresión "atendiendo a la veracidad de la misma" resulta contraria a los artículos 20, 23, 74, 83 y 158 de la Carta**.**

La Corte Constitucional indico en estos párrafos, que, aunque cualquiera podía acceder a esta información, a la hora de difundirla se debía cumplir con la obligación de respetar lo que ella tal cual plasmaba, esto quiere decir, que no se podía modificar esta información, ya que esta debía garantizar la veracidad de lo que en ella se plasmaba.

Con base en este desarrollo normativo y jurisprudencial relacionado en los párrafos anteriores, el Estado se vio en la necesidad de llevar más allá la protección del derecho a la información. Razón está por la cual se expide la Ley 1273 del 2009, esta ley trajo una modificación al código penal, toda vez que incorporó un nuevo bien jurídico tutelado el cual fue denominado de la siguiente forma:

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.**”** Esta modificación al código penal, tuvo en cuenta las el estado actual de la tecnología y como esta estaba influyendo en la sociedad, de esta forma se penalizo las siguientes actuaciones contenidas en la norma. “Artículo 269A: Acceso abusivo a un sistema informático. <Ver Notas del Editor> 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.

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 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, 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.

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.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios

> mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.
>
> Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Modificaciones que fueron muy acordes para el momento que estaba viviendo el país, toda vez que con la gran influencia que estaban teniendo las nuevas tecnologías en el día a día de los integrantes de este país era necesario proteger de alguna forma este medio que es utilizado por muchos y que cada día se apropia más de las actividades cotidianas.

A nivel internacional, varias instituciones se han preocupado por realizar una protección al derecho a la información, dicha protección se puede verificar en lo que se contempló en los cuatro tratados internacionales mencionados a continuación:

> A. Declaración Universal de Derechos Humanos:
>
> Art. 19 – Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.
>
> B. Declaración Americana de los Derechos y Deberes del Hombre:
>
> Art. 4 – Toda persona tiene derecho a la libertad de investigación, de opinión y de expresión, y de difusión del pensamiento por cualquier medio.
>
> C. Pacto de San José de Costa Rica:

ARTÍCULO 13 - LIBERTAD DE PENSAMIENTO Y DE EXPRESION

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura, sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la Ley y ser necesarias para asegurar:

a) El respeto a los derechos o a la reputación de los demás, o

b) La protección de la seguridad nacional, el orden público o a la salud o la moral pública.

3. No se puede restringir el derecho de expresión por vias o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

4. Los espectáculos públicos pueden ser sometidos por la Ley a censura previa con el exclusivo objeto de regular el acceso a ellos para protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

5. Estará prohibida por la Ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a

la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional.

ARTICULO 14 - DERECHO DE RECTIFICACION O RESPUESTA

1. Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio, a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la Ley.

2. En ningún caso la rectificación o la respuesta eximirán de las otras responsabilidades legales en que se hubiese incurrido.

3. Para la efectiva protección de la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial.

D. Conferencia de las Naciones Unidas sobre la Libertad de Información

Art. 1 – Todo individuo tiene derecho a la libertad de pensamiento y a la libertad de expresión sin que pueda haber sobre ello injerencia gubernamental. Este derecho comprende la libertad de opinión, la libertad de investigar, de recibir y de comunicar informaciones e ideas sin consideración de fronteras en forma oral, escrita, impresa e ilustrada o por procedimientos visuales o auditivos legalmente admitidos.

Art. 2 - El derecho a la libertad de expresión trae aparejado deberes y responsabilidades, puede en consecuencia, ser sometido a sanciones,

> condiciones, o restricciones claramente definidas por la ley, pero solamente en lo que concierne a:
>
> a. Las cuestiones que exigen el secreto en interés de la seguridad nacional;
>
> b. Las expresiones de opinión que inciten a cambiar por la violencia el sistema de gobierno;
>
> c. Las expresiones de opinión incitando directamente a cometer actos criminales;
>
> d. Las expresiones obscenas;
>
> e. Las expresiones de opinión que comprometan el curso regular de la justicia;
>
> f. La violación de los derechos existentes en materia de propiedad literaria o artística;
>
> g. Las expresiones de opinión que atenten contra la reputación de otras personas físicas o morales o las perjudiquen de otra manera sin ventajas parta la comunidad:
>
> h. La difusión sistemática de noticias falsas con conocimiento de causa que perjudiquen las relaciones amistosas entre pueblos o Estados. (Declaración universal de derechos humanos)

A nivel de organizaciones que buscan la protección del derecho a la información se encuentra la UNESCO (organización de las naciones unidas para la Educación, la Ciencia y la Cultura) en su página web plasma lo siguiente al hacer una explicación general del tema plasma lo siguiente y el cual citare textualmente:

Acceso a la información pública

La libertad de información ha sido consagrada como corolario de la libertad de expresión en otros instrumentos internacionales importantes, como el Pacto Internacional de Derechos Civiles y Políticos (1966) y la Convención Americana sobre los Derechos Humanos (1969).

La legislación en materia de libertad de información refleja la premisa fundamental de que toda la información en poder de los gobiernos y las instituciones gubernamentales es, en principio, pública y solo podrá ser retenida si existen razones legítimas para no divulgarla, como suelen ser la privacidad y la seguridad.

En los últimos diez años, el derecho a la información ha sido reconocido por una cantidad cada vez mayor de países, incluidos países en desarrollo, a través de la adopción de numerosas leyes sobre libertad de información. En 1990 solo 13 países habían adoptado leyes nacionales sobre libertad de información, mientras que en la actualidad hay más de 90 leyes aprobadas en la materia en países de todo el mundo y hay otras 20 o 30 en estudio.

El mandato de la UNESCO, establecido en su Constitución de 1945, insta específicamente a la Organización a "facilitar la libre circulación de las ideas por medio de la palabra y de la imagen".

La libertad de información es también fundamental en el marco de la Cumbre Mundial sobre la Sociedad de la Información, que ha reafirmado la libertad de expresión y el acceso universal a la información como piedras angulares de las sociedades del conocimiento integradoras.

> Además, la pertinencia de la libertad de información también se ha puesto de relieve en la Declaración de Brisbane sobre libertad de información: el derecho a saber (2010); la Declaración de Maputo: Promover la libertad de expresión, el acceso a la información y la emancipación de las personas (2008) (en inglés) y la Declaración de Dakar sobre medios de comunicación y buena gobernanza (2005), todas ellas resultantes de las conmemoraciones anuales de la UNESCO del Día Mundial de la Libertad de Prensa. (Libertad de información).

En palabras de la UNESCO se puede evidenciar como el derecho a la información debe ser protegido en todo momento y las excepciones que se pueden evidenciar frente a él, como lo son la privacidad (intimidad) y la seguridad. Derechos que, aunque son diferentes, se encuentran ampliamente relacionados.

Es bajo este concepto de protección de la información y su limitación frente a los otros derechos que se ha creado todo un marco normativo en cada país, para proteger los datos personales, una forma de información que a su vez están íntimamente relacionados con el derecho a la intimidad. A nivel internacional los países europeos han sido el referente frente al tema de la protección de datos personales, creando normas para buscar la protección de los datos personales y siendo estos donde el tema de la protección de los datos es una de las muertes a nivel mundial, siendo estos además de referentes para los demás países en la mayoría de los casos los encargados de plantear los lineamientos sobre la protección de los datos adecuada. Se evidencia el nivel de protección que los países de la unión europea manejan frente a los datos personales que en su carta de los derechos fundamentales consagraron como derecho fundamental lo siguiente:

> Artículo 8
>
> Protección de datos de carácter personal
>
> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
>
> 2. Estos 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. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
>
> 3. El respeto de estas normas estará sujeto al control de una autoridad independiente. (Derechos fundamentales de la unión europea).

Con el fin de crear un ambiente de unión entre los países europeos y buscando que este ambiente estuviera enmarcado bajo unos lineamientos de igualdad y protección se expide la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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, tal cual como se indicó el su objetivo plasmando lo siguiente:

> Artículo 1 Objeto de la Directiva
>
> 1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.

Esta directiva fue el punto de partida para que en los países de la unión europea se empezara a elaborar normas buscando la protección de los datos personales teniendo en cuenta los principios contemplados en la directiva, indicaciones plasmadas de la siguiente forma:

Artículo 6

1. Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita;

b) 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;

c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;

d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas 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 rectificados;

e) conservados en una forma que permita la identificación de los interesados durante un período 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 período más largo del mencionado, con fines históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.**”** Principios que han dado las bases para la elaboración de las normas de protección de datos, buscando siempre la protección de los derechos de los titulares, para que no se vulneren sus derechos. En esta Directiva, se hace una división de los datos personales por categorías y como cada una de estas categorías debe tener un tratamiento especial “Artículo 8

Tratamiento de categorías especiales de datos

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

2. Lo dispuesto en el apartado 1 no se aplicará cuando:

a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o

b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o

c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o

d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o

e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.

4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras

> excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.
>
> 5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.
>
> Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.
>
> 6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión.
>
> 7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

Los grandes vínculos comerciales existentes entre la Unión Europea y Estados Unidos ocasionan que entre los dos se dé un flujo de datos a gran escala, transferencia que es necesaria en la era digital en la que vivimos, esto hace que se estén intercambiando entre los dos datos como nombres, apellidos, sexo, estado civil, entre otros. Haciendo con esto necesario que las empresas, tanto de la Unión Europea como de Estados Unidos, garanticen los requisitos mínimos de protección de datos

personales, para poder utilizar los datos que recogen con sus actividades comerciales, producto de esta necesidad, fue creado en conjunto por ambos el escudo de la privacidad, un programa creado para que las empresas cumplan con los requisitos mínimos que estos establecen, permitiendo que de esta forma se realice una trasferencia de datos segura entre las empresas que se encuentran vinculadas al programa.

Como indica la página de la agencia española de protección de datos:

> El 25 de mayo de 2016 entró en vigor el Reglamento General de Protección de Datos (RGPD), que sustituirá a la actual normativa vigente y que comenzará a aplicarse el 25 de mayo de 2018. Este periodo de dos años tiene como objetivo permitir que los Estados de la Unión Europea, las Instituciones y también las empresas y organizaciones que tratan datos vayan preparándose y adaptándose para el momento en que el Reglamento sea aplicable.

Este reglamento entra a derogar la Directiva 95/46/CE, que era el reglamento anterior y por el cual se estaba realizando la protección de los datos personales. Teniendo en cuenta los avances que se generan diariamente, era necesario para la Unión Europea, el actualizar su protección frente a los datos personales para que dentro de toda la unión se garantizara una protección a los datos por parte de los todos los estados miembros. Este nuevo reglamento trajo varias modificaciones, buscando ponerse al día con las exigencias del momento y añadiendo nuevas formas de tratamiento para otros tipos de datos personales que no se habían tenido en cuenta en la directiva anterior. Pero al igual que la directiva anterior, este nuevo reglamento contempla los derechos que los titulares de la información poseen, para que los estados

puedan garantizar una protección efectiva de este derecho. Como punto importante y novedoso, este nuevo reglamento consagró en su artículo 17 lo siguiente:

> Artículo 17
>
> Derecho de supresión («el derecho al olvido»)
>
> 1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:
>
> a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
>
> 4.5.2016 ES Diario Oficial de la Unión Europea L 119/43
>
> b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
>
> c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;
>
> d) los datos personales hayan sido tratados ilícitamente;
>
> e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

En este se plasma como el titular de la información tiene la potestad, en la mayoría de los casos y de apreciar la necesidad, el solicitar al responsable del tratamiento, la eliminación de sus datos, significando esto, además, que los encargados de la información también deben proceder con la supresión de estos datos. Es necesario indicar que esta es la regla general, pero que existen excepciones que impedirían que los datos que el titular de la información solicita sean borrados, en realidad puedan borrarse. Casos como choque con otros derechos, por ejemplo, el de la libertad de expresión e información, cuando estos datos sean de vital importancia para la sociedad que haya un interés público sobre ellos. Un tema muy importante que trae este reglamento y del cual también se había realizado una regulación en la directiva 95/46 se trata de la figura de una autoridad de control, autoridad que cada estado miembro debe contar y que se debe garantizar de realizar la vigilancia a la protección de los datos personales.

Este reglamento también consagro la obligación de la empresa de designar un delegado para la protección de los datos personales plasmado de la siguiente forma:

> Artículo 37 Designación del delegado de protección de datos
>
> 1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que: a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
>
> b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o

fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos

> y a su capacidad para desempeñar las funciones indicadas en el artículo 39.
>
> 6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.
>
> 7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control*.*

Con la creación de esta figura dentro de las empresas responsables y de los encargados del tratamiento de la información para los casos específicos mencionados en la norma, se está buscando la mitigación de los riesgos que general el tratamiento de los datos personales.

El Estado Colombiano, en su búsqueda de proteger la información y, los datos personales, teniendo en cuenta las obligaciones que conlleva el mantenerse actualizado frente al nuevo uso de las tecnologías, las obligaciones que de manera pasiva se generan con la expedición de normas por parte de las grandes potencias, que obligan a los demás países el modernizarse para no quedarse atrás empezó a expedir un cierto número de normas para garantizar el uso correcto de esta información y a su vez limitar el acceso a estos mismos datos.

En nuestro país la protección de un tipo de la información, los datos personales, se vio reflejada con la consagración en el artículo 15 de la constitución política de Colombia que consagro lo siguiente:

> ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos

> respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
>
> En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
>
> La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.
>
> Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

Este artículo que en general se encarga de proteger la privacidad de las personas, toca de manera general la protección frente a los datos, indicando que se respetará la libertad y demás garantías constitucionales cuando se esté realizando una recolección, tratamiento y circulación de estos. Pero fue hasta la creación de la ley 1266 de 2008 que se empezó a ahondar en el tema de la protección de este tipo de información conocido como datos personales. Consagra esta ley en su artículo primero lo siguiente:

> 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 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.

En esta ley, el Estado dando alcance a lo consagrado en el artículo 15 de la constitución estableció unos lineamientos generales frente a la protección de los datos personales y en especial frente al tema de la protección de los datos que se refirieran a la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Esta ley trajo consigo varios principios que se debían respetar a la hora de realizar un tratamiento sobre los datos. Este desarrollo jurídico trajo al país los primeros vestigios a la hora de realizar una protección a los datos, pero no tuvo en cuenta otros aspectos sobre el manejo de los datos, que se estaba evidenciando en el medio y que la ley no reguló Como por ejemplo cuando se realizaba un tratamiento de datos, que no estaban en las centrales de información y que se tenían en bases de datos privadas para temas específicos, por ejemplo en la universidades con el manejo de los datos personales de sus estudiantes, lo cuales eran otorgados en la mayoría de las ocasiones por menores de edad sin capacidad de ejercicio, pero que como la ley no trajo una regulación frente a este aspecto este tipo de dato se recibían y se realizaba el tratamiento que sobre estos se quisiera realizar sin solicitar la autorización por parte de los representantes legales de los menores. Pero es en esta misma ley que se empieza a mencionar el tema de la autorización, dándole la posibilidad, el derecho a las personas, de poder decidir que pasaba con sus datos, las personas podían decidir si querían que su información se entregara a las centrales de información o no.

El Derecho a la protección de datos personales es un derecho autónomo pero que está relacionado ampliamente con los derechos a la intimidad y a la información. En la sentencia C-1011 de 2008 emitida por la Corte Constitucional, se plasmó lo siguiente frente a este aspecto:

> El proyecto de ley estatutaria objeto de examen constituye una regulación parcial del derecho fundamental al hábeas data, concentrada en las reglas para la administración de datos personales de naturaleza financiera, crediticia, comercial, de servicios y la proveniente de terceros países con idéntica naturaleza destinados al cálculo del riesgo crediticio, razón por la cual no puede considerarse como un régimen jurídico que regule, en su integridad, el derecho al hábeas data. El ámbito de protección del derecho fundamental al hábeas data previsto en el Proyecto de Ley, se restringe a la administración de datos de índole comercial o financiera, destinada al cálculo del riesgo crediticio, con exclusión de otras modalidades de administración de datos personales.

Con este análisis la Corte Constitucional dejó claro que esta ley, estaba regulando un aspecto particular del habeas data, aspecto particular directamente relacionado con los tipos de datos personales que trataran sobre temas financieros, crediticios, comerciales y de servicios relacionados con la persona natural que los estaba entregando. Aunque esta ley fue expedida con el objetivo de proteger esos datos en particular, eso no implicó un desconocimiento para la protección de las bases de datos que no fueron tenidas en cuenta por parte de la ley, indicando la corte que este tratamiento de la información seria protegido por el derecho fundamental consagrado en

el artículo 15 de la constitución política y que había sido objeto de desarrollo jurisprudencial por parte de la Corte.

En la sentencia C-1011 de 2008 la Corte plasma que se entiende por HABEAS DATA en el contexto general y que era lo que se estaba regulando hasta el momento plasmando lo siguiente: “El contenido esencial del derecho fundamental al hábeas data radica en el ejercicio efectivo, por parte del sujeto concernido, de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en archivos y bancos de datos”.

De esta forma se evidencio que, aunque la ley 1266 de 2008 estaba realizando una protección sobre los datos personales esta no era de manera general ya que solo se estaba tomando un sector de los datos personales en específico, eso sin indicar que se dejaban los demás datos por un lado y sin protección, pero se evidencio como en este momento histórico era más importante una regulación sobre este tipo de datos que sobre cualquier otro. Sin obviar el hecho de que estos datos personales de tipo financiero pertenecían igualmente al tipo de datos protegidos por el artículo 15 de la constitución política y que simplemente se trataba de una clasificación de estos datos mas no de un nuevo tipo de derecho fundamental individual.

En esta sentencia la Corte Constitucional además plasmo una definición de la información y como esta se podía entender dando además una pequeña definición sobre cada concepto en específico y que indicada de la siguiente forma:

> La jurisprudencia propone dos modos de clasificación de la información: la primera, relacionada con el nivel de protección del derecho a la intimidad, que divide los datos entre información personal e impersonal; la segunda divide los datos personales con base en un carácter cualitativo y según el

> mayor o menor grado en que pueden ser divulgados. Así, se establece la existencia de información pública, semiprivada, privada y reservada.

La Corte hace una distinción de la información desde el punto de vista de su protección y desde un punto de vista cualitativo, este punto de vista cualitativo que divide la información dependiendo de si se trata de información pública, semiprivada, privada y reservada, esta clasificación es las más utilizada en el medio a la hora de desarrollar un tema que involucre el acceso a la información. Por información pública la Corte Constitucional entiende lo siguiente:

> La información pública es aquella que puede ser obtenida sin reserva alguna, entre ella los documentos públicos, habida cuenta el mandato previsto en el artículo 74 C.P. Otros ejemplos se encuentran en las providencias judiciales, los datos sobre el estado civil de las personas o sobre la conformación de la familia. Esta información, puede ser adquirida por cualquier persona, sin necesidad de autorización alguna para ello.

Esta es la primera clasificación de la información, este tipo de información tal como su nombre lo indica es información a la que cualquier persona ya sea natural o jurídica puede tener acceso sin necesidad de contar con la autorización por parte de los dueños de la información

También se plasma la definición de tipo de información como lo es la semiprivada, la cual la Corte Constitucional ha definido de la siguiente manera:

> La información semiprivada es aquel dato personal o impersonal que, al no pertenecer a la categoría de información pública, sí requiere de algún grado de limitación para su acceso, incorporación a bases de datos y divulgación. Por ende, se trata de información que sólo puede accederse

> por orden de autoridad judicial o administrativa y para los fines propios de sus funciones, o a través del cumplimiento de los principios de administración de datos personales. Ejemplo de estos datos son la información relacionada con el comportamiento financiero, comercial y crediticio y los datos sobre la seguridad social distintos a aquellos que tienen que ver con las condiciones médicas de los usuarios.

Este tipo de información es en la cual recae la información de tipo financiero, información que no es pública, pero que por el tipo de información es de interés de grupos específicos, información a la cual no cualquier persona puede acceder libremente, y solo en casos específicos y por órdenes de entidades superiores

Como ultima definición la Corte Constitucional plasma en la sentencia lo siguiente:

> La información privada es aquella que se encuentra en el ámbito propio del sujeto concernido y, por ende, sólo puede accederse por orden de autoridad judicial competente y en ejercicio de sus funciones. Entre dicha información se encuentran los libros de los comerciantes, los documentos privados, las historias clínicas, los datos obtenidos en razón a la inspección de domicilio o luego de la práctica de pruebas en procesos penales sujetas a reserva, entre otros; y por último, la información reservada, que es, aquella que sólo interesa al titular en razón a que está estrechamente relacionada con la protección de sus derechos a la dignidad humana, la intimidad y la libertad; como es el caso de los datos sobre la preferencia sexual de las personas, su credo ideológico o político, su información genética, sus hábitos, etc. Estos datos, que han sido agrupados por la jurisprudencia bajo la categoría de información sensible, no son

> susceptibles de acceso por parte de terceros, salvo que se trate en una situación excepcional, en la que el dato reservado constituya un elemento probatorio pertinente y conducente dentro de una investigación penal y que, a su vez, esté directamente relacionado con el objeto de la investigación. En este escenario, habida cuenta la naturaleza del dato incorporado en el proceso, la información deberá estar sometida a la reserva propia del proceso penal. En la categoría de datos privados, el legislador estatutario ha englobado las categorías de información privada y reservada.

Este tipo de información es muy importante y sin duda es el tipo de información al que más atención se le debe prestar, toda vez que se trata de los datos privados o reservados, son aquel tipo de información que por su contenido solo le interesa al titular de ella, o aquel tipo de información que de ser llegada a difundir por algún tercero podría resultar en un detrimento para los demás derechos del titular, dentro de esta categoría se encuentra como un claro ejemplo las preferencias sexuales, este tipo de información que podría llevar a un perjuicio del titular de la misma y la cual no se está en la obligación de ser conocida por algún tercero.

Pero como se garantizar que los datos personales que fueron adquiridos por lo bancos de información, por las centrales de información, si recibirían el tratamiento adecuado y acorde a los derechos que poseen los titulares de la información, la ley tuvo en cuenta este aspecto y por eso plasmo una serie de derechos que las personas, tanto jurídicas como naturales posen los cuales fueron indicados en la sentencia C- 1011 de 2008 y son los siguientes, encontrándose en esta además la definición del titular de la información :

La definición del titular de la información, como aquella persona natural o jurídica a quien se refiere la información que reposa en un banco de datos, le otorga al titular la condición de sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere el Proyecto de Ley, siendo tanto las personas naturales como jurídicas susceptibles de producir información que puede ser recolectada por las bases de datos, lo que impone el deber de otorgar un nivel de protección suficiente y adecuado a esa información personal, y dado que el Proyecto de Ley está relacionado con la administración de datos de contenido financiero, comercial y crediticio, resulta innegable que las personas jurídicas son participantes indiscutibles del mercado comercial y de crédito, de modo tal que resultaría injustificado excluirlas de las garantías que se predican a favor del titular de información de esta naturaleza. Frente a los operadores de los bancos de datos, los titulares de la información podrán (i) ejercer el derecho fundamental al hábeas data, mediante la utilización de los procedimientos de consultas o reclamos, sin perjuicio de los demás mecanismos constitucionales y legales; (ii) 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; (iii) solicitar prueba de la certificación de la existencia de la autorización expedida por la fuente o por el usuario; y (iv) solicitar información acerca de los usuarios autorizados para obtener información. Ante la fuente de información, teniendo éstas el deber de notificar al titular sobre la intención de enviar información sobre

> incumplimiento a los operadores, los titulares tienen el derecho de ejercer los derechos fundamentales al hábeas data y de petición, procedimientos que (i) podrán cumplir a través de los operadores de información, mediante los trámites de consultas y reclamos dispuestos en la norma estatutaria; y (ii) operan sin perjuicio de la vigencia de los demás mecanismos constitucionales o legales.

De esto se puede apreciar que esta ley, no solo tuvo en cuenta solo la información generada por las personas naturales, además pensó también en la información generada por las personas jurídicas, dotando de protección también a la información que estas generaran concerniente a los aspectos relacionados con los datos de contenido financiero, comercial y crediticio. Y es interesante el análisis en el cual incurre la corte al reconocer que como las personas jurídicas producen información del tipo ya mencionado, son sujetos que jurídicamente deben ser cobijados por este derecho fundamental del habeas data, por consiguiente, ser protegidos por esta ley estatutaria.

En estos derechos se le indico a la titular de la información, la manera como poder hacer eso de su derecho fundamental, que mecanismos podía ejercer para que la información la cual entregó y que se estaba almacenando por las centrales de riesgo fueran protegidas por estas, garantizándole la seguridad de saber que sus datos personales estarían seguros.

Por varios años la ley 1266 de 2008 fue la ley encargada de regular el tema de protección de datos personales, pero como ya fue mencionado en párrafos anteriores, esta ley se enfocó en unos datos personales en específico, los datos personales de tipo comercial, financiero y crediticio, sin dejar a un lado los demás grupos de información, pero no dándole una regulación especial.

En el año 2012 con la expedición de la ley 1581, se empieza a evidenciar la necesidad del Estado de afrontar la realidad que se empieza a evidenciar con el manejo de los datos personales, toda vez que con la entrada en operación de las redes sociales y el uso de los medios electrónicos, se hace necesario el proteger los datos personales de las personas, esto por el riegos que se estaban presentando con estos medios tecnológicos además del hecho de buscar con esto una regulación general sobre la protección de datos personales que con la expedición de la ley 1266 de 2008 no fue regulada en su totalidad, es importante indicar la diferencia que existe entre las dos normas en el hecho de que la ley 1266 de 2008, además de proteger a las personas naturales, también protegió a las personas jurídicas, por generan estas datos comerciales, financieros y crediticios, pero a diferencia de esta ley, la 1581 de 2012 solo protege los datos de las personas naturales, es por esta razón que la ley 1581 no entro a derogar los temas plasmados en la 1266, dejando con vigencia a la primera, toda vez que esa estaba regulando temas de manera especializada.

La ley 1581 de 2012 trajo como objetivo el siguiente:

> 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 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.

La protección de esta ley está para cualquier base de datos o archivo que recogiera información de una persona buscando garantizar el cumplimiento de los

derechos contenidos en la misma. Por ese motivo es que más adelante se creara el registro nacional de base de datos, buscando dar aplicación a la norma indicada, buscando la efectividad de la misma y que de una forma u otra se pueda cumplir con la protección de los datos personales.

La sentencia C-748 de 2011 se encargó del control constitucional de la ley 1581 de 2012, en esta sentencia la corte indico las definiciones que a través del tiempo habían afrontado para la definición de habeas data y las cuales son las siguientes:

> 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. También, desde los primeros años de la nueva Carta, surgió al interior de la Corte una segunda línea interpretativa que consideraba el habeas data una manifestación del libre desarrollo de la personalidad. 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. Ya a partir de 1995, surge una tercera línea interpretativa que es la que ha prevalecido desde entonces y que apunta al habeas data como un derecho autónomo, en que el núcleo del derecho al habeas data está compuesto por la autodeterminación informática y la libertad –incluida la libertad económica. 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.

La Corte Constitucional también menciono lo ya dicho anteriormente frente a la ley 1266 de 2008 y como esta, aunque trato de ser una ley de protección general de datos personales, al final terminó enfocándose en un tipo de datos en específicos, los datos financieros, comerciales y crediticios:

> En el caso colombiano, el proyecto de ley que dio lugar a la Ley 1266 de 2008 y que fuera objeto de la sentencia C-1011 de 2008, buscaba convertirse en una ley de principios generales aplicable a todas las categorías de datos personales, pero pese a su pretensión de generalidad, el proyecto de ley en realidad solamente establecía estándares básicos de protección para el dato financiero y comercial destinado a calcular el nivel de riesgo crediticio de las personas. Por ello en la referida sentencia, la Corte dejó claro que la materia de lo que luego se convertiría en la Ley 1266 es solamente el dato financiero y comercial. Por lo tanto, la Ley 1266 solamente puede ser considerada una regulación sectorial del habeas data.

La Corte Constitucional pone en evidencia la amplia relación que existe entre el derecho al habeas data y el derecho a la privacidad y al derecho de la libertad de

información consagrado en el artículo 20 de la constitución política de Colombia, derecho que consagra lo siguiente:

> ARTICULO 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.
>
> Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

Buscando que de esta forma se esté garantizando el derecho de cualquier titular de la información de hacer con esta lo que quiera y de que se haga con esta lo que este autorice siempre y cuando sea algo legal. En la sentencia por la cual se le hizo el control de constitucionalidad a la ley 1581 de 2012, se indicó por parte de la corte constitucional cuales tiene que ser las garantías mínimas que debe contener cualquier regulación sobre habeas data y las cuales fueron identificadas así:

> 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 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 rectificada o corregida, 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.

Estos son los requisitos mínimos que debe de tener cualquier regulación y son los requisitos que se deben de tener en cuenta por la entidad encargada de realizar la protección de datos personales a la hora de realizar una vigilancia sobre la protección de datos personales.

Los operadores jurídicos tuvieron en cuenta varios modelos de protección de datos los cuales la Corte menciono en la sentencia y los cuales son los siguientes:

> 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 propio 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.

Pero aun así el estado colombiano aplico un modelo híbrido que la Corte Constitucional define de la siguiente forma:

> Ahora, con el nuevo proyecto de ley se busca llenar el vacío de estándares mínimos de protección de todos los datos personales, de ahí que su título sea precisamente “Por el cual se dictan disposiciones generales para la protección de datos personales”, concluyéndose que 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.

De esta forma el Estado Colombiano protege todos los datos personales de una manera general, indicando las obligaciones mínimas que se deben de tener en cuenta a la hora de realizar un tratamiento de datos personales, a su vez es el punto de partida para cuando se necesite realizar un tratamiento sobre datos personales que de una u otra forma son datos de mayor importancia.

Los temas regulados en la ley 1581 de 2012, en su mayoría fueron aportados por los planteamientos normativos que la Unión Europea había diseñado para los estaos miembros, razón está por la cual esta norma es muy parecida a el marco europeo de protección de datos personales. La influencia de la normativa europea, se puede evidenciar con la creación de la delegatura para la protección de datos personales de la Superintendencia de Industria y Comercio, entidad que se encargó de la creación del registro nacional de base de datos, registro que tiene por objetivo el registrar las bases de datos de todas las entidades jurídicas que manejen datos personales, para de esta forma llevar un control y vigilancia sobre ellos. Este registro trae consigo la obligación de cumplir lo estipulado en la ley 1581 de 2012, frente al tema de proteger los derechos de los titulares, la creación de las políticas de tratamiento de los datos personales, contar con la autorización de los titulares de la información, contar con las medidas de seguridad adecuadas considerando el tipo de datos que se estén manejado. Esta obligación quedo plasmada de la siguiente manera:

> CAPÍTULO III.
>
> DEL REGISTRO NACIONAL DE BASES DE DATOS.

> ARTÍCULO 25. DEFINICIÓN. El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país.
>
> El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.
>
> Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley.
>
> PARÁGRAFO. El Gobierno Nacional reglamentará, dentro del año siguiente a la promulgación de la presente ley, la información mínima que debe contener el Registro, y los términos y condiciones bajo los cuales se deben inscribir en este los Responsables del Tratamiento.

Aunque este registro estuvo plasmado desde el año 2012, fue tiempo después, que se creó por parte de la Superintendencia de Industria y Comercio el sistema para que las empresas jurídicas pudieran empezar a registrar sus bases de datos. Aunque se les ha dado una fecha límite a los responsables de la información, la misma se ha modificado en varias ocasiones por la falta de registro por parte de los obligados. Este registro busca además el reconocimiento de los derechos de los titulares de la información, al permitirles conocer las obligaciones que tienen los responsables de la información, conociendo así la posibilidad que tiene de decidir, en la mayoría de los casos, el destino de sus datos personales.

Mediante la expedición de la sentencia de tutela 176A de 2014 la Corte Constitucional estableció lo siguiente frente al derecho al habeas data:

> En resumen, el reconocimiento del derecho fundamental autónomo al habeas data, busca la protección de los datos personales en un universo globalizado en el que el poder informático es creciente. Esta protección responde a la importancia que tales datos revisten para la garantía de otros derechos como la intimidad, el buen nombre, el libre desarrollo de la personalidad, entre otros. Sin embargo, el que exista una estrecha relación con tales derechos, no significa que no sea un derecho diferente, en tanto conlleva una serie de garantías diferenciables, cuya protección es directamente reclamable por medio de la acción de tutela, sin prejuicio del principio de subsidiariedad que rige la procedencia de la acción.

Metodología

El desarrollo del trabajo es de carácter descriptivo, toda vez que se pretende evidenciar la realidad social que atraviesa Colombia frente a la protección de los datos personales y los impactos de la ley 1581 en los demás derechos. Concretamente este trabajo, pretende tratar el efecto que genera cuando se presentan conflictos respecto al derecho a la libertad de información permitiendo de esta forma una posible predicción del enfoque que el Estado le ha dado al objetivo de estos derechos y cómo será su implementación a futuro.

Conclusiones

Colombia como un país que busca su evolución constante, requiere el no quedarse atrás con los avances que a nivel internacional se realizan en todos los aspectos de un mundo globalizado, aspectos que tiene que ver tanto con avances tecnológicos, implementación de nuevas tecnologías, como con la creación e implementación de normas que regulen estas tecnologías. Como se ha podido evidenciar cada año, el uso de la tecnología y de las aplicaciones que permitan conectar una persona con otra está en aumento, desde el uso del MSN en el pasado, hasta el uso de Facebook y WhatsApp hoy en día. Aplicaciones que permiten el intercambio de información desde una persona de un país con otra en otro país totalmente alejado. Envío de información que no se limita por las grandes distancias que tiene que recorrer ni por las fronteras que separan los países, nace con esto la necesidad de que la información que se comparte sea protegida tanto por el país que la envía, como por el país donde va a ser recibida.

Razón está por la cual el Estado colombiano ha creado varias normas para la protección de la información, en especial de los datos personales, normas creadas en su mayoría teniendo como modelo las creaciones normativas de otros países, como se pudo evidenciar con la creación del registro nacional del base de datos en cabeza de la Superintendencia de Industria y Comercio. Registro que fue tomado de lo plasmado por la Unión Europea para lo protección de los datos en el territorio europeo, pero que sin duda no fue analizado en su totalidad a la hora de implementarse en nuestro país, toda vez que dicho registro requiere de un acceso a la tecnología constante, dejando de lado todos aquellos que no pueden acceder ni siquiera a un computador, mucho menos a internet.

Pero sin quitarle demeritar la finalidad de la ley 1581 de 2012, se debió haber realizado un estudio y planeación para la implementación de dicha norma en nuestro país, para que de esta forma la protección de los datos personales fuera una protección para todo un país y no para unos cuantos con acceso a las comodidades tecnológicas de hoy en día.

Dicho modelo e implementación debería ser estudiado por la academia, donde se permita que esta regulación para la protección de los datos personales no solo sea para unos pocos, sino que pueda abarcar a todos los habitantes del territorio colombiano. Creación normativa que debería contener en su interior el análisis de su relación con el derecho a la información y como limita uno al otro. Estudio necesario para la creación de una nueva normativa para regular este tema de protección de datos personales, esto teniendo en cuenta que el modelo utilizado por Colombia, basado casi en su totalidad del de la Unión Europea ya ha sido reformado por la misma Unión Europea al no generarle los resultados esperados, razón está por la que Colombia debería plantear si desea copiar de nuevo la nueva creación de la Unión Europea o decidirse ella misma a crear su propia normativa teniendo en cuenta las realidades de este país.

Referencias

Agencia Española de Protección de Datos. (2017). *Reglamento general de protección de datos.* Recuperado de http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php

Asamblea General de las Naciones Unidas. (1948). Declaración Universal de Derechos Humanos. París: Naciones Unidas.

Asamblea Nacional. (1789). Declaración de los Derechos del Hombre y del Ciudadano. Francia: Asamblea Nacional.

Asamblea Nacional Constituyente. (1991). Constitución Política de Colombia. Bogotá: Asamblea Nacional Constituyente.

Comisión Interamericana de Derechos Humanos. (1948). Declaración Americana de los derechos y deberes del hombre. Bogotá, Colombia. Comisión Interamericana de Derechos Humanos.

Congreso de La República. (2008). Ley Estatutaria 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. Bogotá: Congreso de la República.

Congreso de La República. (2009). 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. Bogotá: Congreso de La República.

Congreso de La República. (2009). Ley 1341 de 2009, Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Bogotá: Congreso de La República.

Congreso de La República. (2012). Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá: Congreso de La República.

Congreso de La República. (2014). Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Bogotá: Congreso de La República.

Corte Constitucional de Colombia. (1992). Sentencia T-609 de 14 de diciembre de 1992. Magistrado ponente Fabio Morón Díaz. Colombia.

Corte Constitucional de Colombia. (2008). Sentencia C- 1011 de 16 de octubre de 2008. Magistrado ponente Jaime Córdoba Triviño. Colombia.

Corte Constitucional de Colombia. (2011). Sentencia T-161 de 10 de marzo de 2011. Magistrado ponente Humberto Antonio Sierra Porto. Colombia.

Corte Constitucional de Colombia. (2011). Sentencia C-748 de 6 de octubre de 2011. Magistrado ponente Jorge Ignacio Pretel Chaljub. Colombia.

Corte Constitucional de Colombia. (2013). Sentencia C-274 de 9 de mayo de 2013. Magistrada ponente María Victoria Calle Correa. Colombia.

Corte Constitucional de Colombia. (2014). Sentencia T-176A de 25 de marzo de 2014. Magistrado ponente Jorge Ignacio Pretel Chaljub. Colombia.

Milton, Jhon. (2000). *Areopagítica*. México: Fondo de cultura Económica.

Organización de las naciones Unidas para la Educación, la Ciencia y la Cultura. (2017). *Libertad de información*. Recuperado de http://www.unesco.org/new/es/communication-and-information/freedom-of-expression/freedom-of-information/

Organización de los Estados Americanos. (1969). Convención Americana sobre derechos humanos. San José de Costa Rica: Organización de los Estados Americanos.

Parlamento Europeo, el Consejo y la Comisión. (2007). Carta de los derechos fundamentales de la Unión Europea. Estrasburgo: Unión Europea.

Parlamento Europeo y del Consejo de la Unión Europea. (1995). Directiva 95/46/CE del Parlamento Europeo y del Consejo. Luxemburgo: Unión Europea.

Tzu, Sun. (2003 versión), *El arte de la guerra.* Recuperado de http://www.biblioteca.org.ar/libros/656228.pdf