PROTECCIÓN DE DATOS PERSONALES EN TIEMPOS DEL BIG DATA

Saray Vanessa Barbosa Salgado

Dirigido por:

Diana Carolina Valencia Tello

Presentada como requisito para optar por título de

Máster en Derecho con énfasis en Público en la Facultad de Jurisprudencia

Universidad Colegio Mayor de Nuestra Señora del Rosario

Semestre II, 2022

TABLA DE CONTENIDO

Resumen

El Big Data consiste en el procesamiento de grandes volúmenes de información, que puede provenir de múltiples fuentes y estar en diversos formatos, para generar análisis que pueden describir el estado de una organización en tiempo real, así como detectar correlaciones que permitan predecir con cierto grado de certeza una situación o tendencia incidiendo en la toma de decisiones mediante el procesamiento de información histórica. Por ello, en el presente documento se analizará el régimen de protección de datos personales que rige a este procesamiento de información.

Palabras claves: datos, protección de datos, habeas data, Big Data, contrato, transferencia de datos, autorización.

Abstract

Big Data consists of the processing of large volumes of information that can come from multiple sources and in various formats, to generate analytics that describe the real-time status of an organization, as well as by processing historical information to detect correlations. that allow predicting with a certain degree of certainty a situation or trend influencing decision-making. For this reason, this document will analyze the personal data protection regime that governs this information processing.

Key words: data, privacy, habeas data, Big Data, contract, transference, authorization

1. Introducción

Chaves (2004) define una revolución industrial como un proceso y no como un evento, a partir de la definición de primera revolución industrial del profesor David S. Landes, a saber:

"*El término revolución industrial suele referirse al complejo de innovaciones tecnológicas que, al sustituir la habilidad humana por la maquinaria y la fuerza humana y animal por energía mecánica, provoca el paso desde la producción artesana a la fabril, dando así lugar al nacimiento de la economía moderna*".

Las asimetrías territoriales, económicas, políticas y tecnológicas entre los países explican por qué estas revoluciones se han desarrollado en diferentes periodos de tiempo entre ellos, al punto que mientras en la primera mitad del siglo XX en países no desarrollados se consolidaba la primera y segunda revolución, en los más desarrollados la segunda guerra mundial sentaba las bases de la tercera revolución industrial. Esta afirmación se hace tomando como referencia que en cada una de estas *revoluciones* hay una innovación que es fijada como el punto de evidencia de la consolidación de los cambios históricos. Es el caso de Davis (2016), quien postula la invención de la máquina de vapor en 1784 como punto de partida de la primera revolución industrial, la división del trabajo, electricidad y producción de masa como innovaciones protagonistas de la segunda revolución industrial a partir de 1870 y la electrónica e informática, así como la producción automatizada como punto coyuntural de la tercera revolución industrial en 1969.

De esta tercera revolución vale la pena destacar que la segunda guerra mundial creó las condiciones para que los Estados más desarrollados enfocaran su inversión no sólo en armas sino en invenciones de tipo más estratégico, como la Bombe, creada por Alan Turing para que el Gobierno británico pudiese descifrar las comunicaciones alemanas que eran cifradas por Enigma, una máquina que cambiaba el código cada día. Creada por el ingeniero alemán Arthur

Scherbius, la Bombe usaba electricidad para poner en marcha deducciones lógicas descartando las combinaciones no coincidentes, llegando al punto de decodificar dos mensajes por minuto, logrando reemplazar con una máquina el trabajo de los criptógrafos humanos y sentando así las bases de la computación. (Sadurní, 2021)

Esta última actividad, que se vio facilitada y fortalecida en la década de los setenta, donde los desarrollos tecnológicos fueron impulsados desde actores del sector privado con fines de lucro, y no en la defensa de los Estados, como había ocurrido en las dos décadas precedentes. Este cambio de enfoque incidió directamente en la velocidad con la que se fueron produciendo mejoras tecnológicas, como aumentos en la apropiación, capacidad, velocidad o disminución en los tamaños y precios de los dispositivos tecnológicos, fomentando la masificación gracias al afán de captar mayor clientela (Castells, 2006). Debido a esta masificación, Valencia (2015) describe la tercera revolución industrial como la era de la globalización y las nuevas tecnologías, pues esta etapa histórica se caracteriza por el fortalecimiento del mercado debido a los avances tecnológicos y científicos hasta el punto de la consolidación de intervinientes en el mercado que igualan o superan el poder económico y político de los Estados, que permiten percibir un debilitamiento desde el punto de vista de su soberanía, dado que se han visto obligados a cooperar en el marco de organizaciones internacionales para poder llegar a acuerdos e implementar regulaciones a estos actores del sector privado.

Además de la diversificación de los intervinientes en el plano internacional, estas tecnologías han generado una ampliación del acceso y creación de la información disponible para los ciudadanos, así como la disponibilidad de diversas redes para relacionarse. Así, permiten encontrar puntos de vista diferentes o puntos de vista similares en diferentes realidades, pero el acceso a ese gran volumen de información también ha dado origen a riesgos individuales o masivos de daños irreparables o gravemente onerosos.

Estos cambios han generados tensiones con los individuos, quienes, a pesar de verse directamente beneficiados con las bondades tecnológicas de la computación, internet y tecnología, también son vulnerables en aspectos que antes no se concebían. En efecto, su información personal pasó de ser parte de su esfera íntima a ser manejada por el Estado, particulares e incluso organizaciones extranjeras. De ahí que desde 1966, en el seno de la Organización de Naciones Unidas, se consagrara la importancia de la privacidad y regular el uso que se da a la información de las personas. (Asamblea General de las Naciones Unidas, 1968)

Esta preocupación ha derivado en la progresiva regulación del tratamiento de datos personales a escala nacional e internacional, así como iniciativas de políticas de autorregulación por parte de los intervinientes en el mercado que tratan datos personales de forma global y deben dar cuenta de diferentes niveles de cumplimiento ante la autoridad de protección de datos de cada país, que desee tratar datos personales de sus ciudadanos. Estas regulaciones, como se verá más adelante, se erigieron sobre un supuesto y es que el individuo conoce su información y la entrega, con autorización, para que sea tratada por otras personas bajo los límites que el individuo y la legislación aplicable exijan.

Estos nuevos retos han impulsado la percepción de que desde 2016 se está experimentando una cuarta revolución industrial. Esta fue inicialmente planteada por Klaus Martin Schwab, presidente del Foro Económico Mundial, autor del libro *La cuarta revolución industrial* (Schwab, 2016) y fundador en 1971 de esta organización internacional que promueve la cooperación entre agentes públicos y privados atribuyéndose imparcialidad política, pero con el objetivo de disminuir la desigualdad y lograr el balance de la economía mundial. (Foro Económico Internacional, s.f.)

Shwab (2016) señala que son varias las tecnologías que son referentes de la apropiación de la cuarta revolución industrial. Entre ellas podemos encontrar el Big Data, la inteligencia artificial (IA), la robótica, el internet de las cosas (IoT), los vehículos autónomos, la impresión 3D, la nanotecnología, la biotecnología, la ciencia de materiales, el almacenamiento de energía, entre otros, que superan lo ya alcanzado con los referentes tecnológicos de la tercera revolución industrial, esto es el internet y la computación, pues las precitadas innovaciones conllevan cambios digitales, físicos y biológicos, que no cambia lo que se hace (en términos de industria o mercado), sino la esencia de lo que son los seres humanos.

En consideración a que la legislación vigente fue emitida en el contexto de la tercera revolución industrial es pertinente revisar si la regulación de protección de datos personales creada en vigencia de la era anterior es eficaz ante las nuevas circunstancias. Para ello se concentrará el análisis en el marco de uno de los desarrollos tecnológicos más relevantes de esta nueva etapa: el Big Data.

Este adelanto tecnológico no solamente se refiere al procesamiento de grandes volúmenes de datos o Macrodatos sino a la implementación de un conjunto de herramientas digitales que permiten analizar en tiempo real estos datos para convertirlos en información. Tal conversión es el resultado de análisis que no solo describen los datos, sino la posibilidad de que se emitan predicciones sobre el comportamiento de los sujetos sobre los que se refiere la información, la cual se hace con data estructurada como hojas de cálculo, archivos de texto o bases de datos, y también permite el análisis con datos no estructurados como imágenes en diversos formatos, videos, publicaciones de redes sociales o datos de internet de las cosas, como relojes inteligentes. (Barranco Fragoso, 2012)

La información resultante que puede guiar la toma de decisiones inmediatas sobre las organizaciones, sus servicios, productos y, particularmente, sobre las personas, pasando así el

individuo de ser un beneficiario de la información a convertirse en una fuente de ésta, aun cuando no sea consciente de ello. (Oracle Colombia, s.f.)

En ese sentido, este trabajo presentará la regulación de protección de datos vigente en Colombia, sus antecedentes y desarrollo. Posteriormente, se caracterizará la cuarta revolución industrial centrándose en qué es Big Data y sus aplicaciones, así como sus interacciones con los individuos en relación con la protección de datos personales, para finalizar con la descripción del esfuerzo internacional y extranjero, ante en materia de protección de datos personales.

2. Capítulo I - Derecho fundamental a la protección de datos personales en Colombia

2.1 Antecedentes

De acuerdo con lo expuesto por diversos autores, entre ellos Chaves (2004) los procesos de revolución industrial llegan de forma diferenciada según el desarrollo de los países, en ese sentido para la primera y segunda revolución el pionero fue el Reino Unido, expandiéndose luego a los demás países europeos y, posteriormente, Estados Unidos, cuyo desarrollo tecnológico toma protagonismo, a partir del lanzamiento de las bombas atómicas que arrasaron con Hiroshima y Nagasaki dando fin a la segunda guerra mundial (Valencia, 2015).

Colombia durante la primera revolución industrial era parte del Reino de la Nueva Granada, es decir colonia española. Nuestro país no estuvo a la vanguardia del desarrollo industrial, pues su bonanza era producto de la extracción de recursos de sus colonias. Luego de su independencia (proceso que se surtió entre 1810 a 1819) se vio en vuelta en conflictos internos que dieron lugar a una inestabilidad jurídica, política y económica cambiando sucesivamente de gobiernos, constituciones y forma de Estado, de manera que sólo llegó a un momento de estabilidad hasta el final de la guerra civil de 1885, momento en que se logró convocar a un Consejo Nacional de Delegatarios que dio origen a la llamada Constitución de 1886, caracterizada por implementar un Estado de Derecho, centralista y unitario, inspirado en la República Francesa (Olano, 2019). Así las cosas, solo hasta finalizada la Guerra de los Mil Días empezó a dejar de ser suntuosa la idea de invertir en crear industria en Colombia.

Este siglo de sucesivos conflictos tuvo un alto costo para el desarrollo científico, tecnológico e industrial de Colombia, al punto que, para inicios del siglo XX, compartía con Haití el más bajo escalafón en inversión extranjera, ferrocarriles y sólo lograba exportar el 36% más de lo que exportaba cuando era colonia. Así mismo, se caracterizaba por tener sistemas de

producción atrasados y una geografía compleja (Echavarría, Villamizar, & González), mientras Europa ya finalizaba la segunda revolución industrial y empezaba a crear las bases de la tercera.

A partir del fin de la Segunda Guerra Mundial se inicia una pugna entre Estados Unidos y Rusia por el desarrollo tecnológico y armamentista, periodo que se conoce como "Guerra Fría", caracterizado por la ausencia de conflictos directos entre estas dos potencias, pero sí una serie de conflictos internos en otros países, promovidos por los modelos económicos antagónicos que ambas representaban. Este periodo de pugna sirvió como incentivo para la creación de tecnologías que hoy son de uso doméstico pero que entonces nacían para uso militar y restrictivo como los computadores, esquema que empieza cambiar a partir de 1950 con la UNIVAC, la primera computadora de uso comercial que se usó para procesar los datos del censo de Estados Unidos. (Hernández, 2011).

De forma paralela, el reto para Colombia fue ponerse al día en dos siglos de revoluciones industriales mediante la implementación de otros medios de transporte y energía, así como la conformación de grandes industrias y plantas que permitieran participar en el mercado (Echavarría, Villamizar, & González), mientras esta nueva industria procuraba nacer y crecer trayendo lo último en tecnología al país. Ejemplo de ello fue Bavaria, empresa que trajo a Colombia la primera computadora el 3 de marzo de 1957. Se trataba de una IBM 650, conocida por ser la más comercializada de las computadoras de primera generación. (Revista Semana, s.f.)

Antes de que el Estado colombiano se preocupara por regular y vigilar el uso de la información, cuando esta se refiere a personas, el sector privado del mercado colombiano poco a poco se unía a la tendencia mundial de ejecutar actividades como recolección, uso, circulación o supresión de datos personales con distintos fines. Ejemplo de ello fue la creación en 1964 de la Central de riesgos del sector financiero (CIFIN), con el propósito de centralizar, organizar y

compartir el estado de riesgo y endeudamiento de los usuarios del sector financiero (Asociación Bancaria y de Entidades Financieras de Colombia, s.f.).

A pesar de que la apropiación de las tecnologías ha sido un proceso lento para Estados como el colombiano, una de las características de la era de la globalización y las nuevas tecnologías consiste en que las empresas de alta tecnología y las sociedades financieras extendieron su alcance de forma global. Así las cosas, IBM llegó a Colombia entre 1980 a 1983. Para diciembre de 1987 existían 640 empresas oficiales que procesaban datos, mientras 2.535 empresas lo hacían en el sector privado, de acuerdo con el censo realizado por el DANE (Sentencia T-414, 1992). En 1988 llegaría al país la primera computadora personal (Compaq 386), tan solo un año después de su lanzamiento en Estados Unidos y dos después de que el mercado estadounidense viviera el auge de las computadoras personales. (El Tiempo, 2008)

De ahí que, en 1987, por solicitud de la Presidencia de la República, la Universidad de los Andes formuló un Proyecto de ley de protección de datos personales, fruto del trabajo interdisciplinar entre el "Centro de Investigación de la Facultad de Ingeniería" y la Facultad de Derecho. En él se recogen los desarrollos legislativos de otros países, entre los que se encuentra la obligación de designar una autoridad administrativa a cargo de la vigilancia y control de las bases de datos. En esta propuesta se sugiere la creación de una entidad inspirada en la Comisión de Valores y en la Comisión Nacional de Televisión que funja como autoridad de protección de datos personales. En relación con el ámbito de aplicación del proyecto se reconoce como titular de datos personales a personas naturales y jurídicas por igual, fijando como pilar para el tratamiento de datos la autorización, y propone un registro de bases de datos. Lamentablemente este proyecto no llegó a ser ley. (Losano, 1989)

A pesar del fracaso de dicho proyecto, las actividades de recolección, almacenamiento y procesamiento de datos estaban permitidas bajo presunción de legalidad, en virtud de lo

consagrado en el artículo 20 de la Constitución Política de 1886, que les permitía a los particulares ser responsables por infringir aquello que prohibiera la Constitución y la Ley. En ese sentido, la falta de regulación sobre el derecho a la protección de datos persones dotaba de validez toda actividad que no estuviese expresamente prohibida.

No obstante, la ausencia de una norma jurídica que describiera y regulara esta actividad implicó una desprotección de los individuos titulares de la información, ya que no existían entidades administrativas o jurisdiccionales con la competencia para declarar y sancionar conductas ilegitimas, como puede ser el inadecuado uso de la información personal, la divulgación de información o la información incompleta. Esta situación fue subsanada una vez entró en vigencia la Constitución Política de 1991 y, en particular, las garantías fundamentales establecidas en el artículo 15, susceptibles de ser protegidas judicialmente a través de la acción de tutela consagrada en el artículo 86.

En este orden de ideas, el derecho de protección de datos personales fue consagrado en Colombia con la Constitución Política de 1991. El proyecto de acto reformatorio presentado por el ejecutivo reconoce la necesidad originada por los desarrollos tecnológicos de la época, de dotar a las personas naturales y jurídicas de un derecho que implicara no sólo la posibilidad de conocer la información que reposa de sí mismas en bases de datos, sino también, que se abriera la posibilidad de corregirla, eliminarla y actualizarla, de suerte que se materializara un derecho de “autodeterminación” informática. (Cifuentes Muñoz, 1997).

La discusión en torno la consagración de este derecho no giró por la existencia de opositores a su inclusión en el texto constitucional, pues para la época centrales de riesgo como CIFIN cumplían más de 20 años ejerciendo tratamiento de datos personales sin una entidad que vigilara el ejercicio de la actividad o un procedimiento judicial idóneo contra los conflictos que pudiesen suscitarse en el marco de la misma. En particular, si se tiene en cuenta que éstas

centrales de riesgo tenían un vínculo contractual con las entidades financieras pero no un vínculo con los ciudadanos, que no tenían a quién acudir, como se reconoce en la primera sentencia que abordó la vulneración a este derecho la T-414 (Sentencia T-414, 1992)

El debate en la Asamblea Nacional Constituyente giró en torno a las múltiples propuestas de redacción de su contenido, entre las que Remolina (Tratamiento de Datos Personales. aproximación internacional y comentarios a la Ley 1581 de 2012, 2013) destaca en primera medida: la presentada por María Mercedes Carranza y Francisco Rojas Birry, quienes propusieron el uso de la expresión "habeas data". Si bien esta expresión no se incorporó en el articulado, sería usada posteriormente por la jurisprudencia constitucional para referirse al "régimen de protección de datos personales de Colombia", teniendo en cuenta la ausencia de una acción judicial especializada en estos asuntos, como existe en otras legislaciones, según se verá más adelante.

En segunda medida, Remolina destaca la propuesta presentada por Guillermo Perry Rubio, quien formuló el uso de la expresión libertad informática, lamentablemente sin explicar su alcance. Al respecto, el segundo inciso del artículo constitucional incluye el principio de libertad como uno de los ejes rectores de este derecho fundamental, cuyo contenido es ampliado por desarrollo jurisprudencial.

En tercera medida, Remolina describe que el constituyente Jaime Álvaro Fajardo propuso que desde esta disposición se ordenara la reglamentación legislativa del uso de la informática y de otros "avances tecnológicos". Esta propuesta no llegó a incorporarse en la redacción final del derecho, manteniendo así la presunción de legalidad, vigente desde la Constitución de 1886.

Luego, en cuarto lugar, Remolina señala que en la propuesta presentada por Alfredo Vásquez Carrizosa y Misael Pastrana Borrero se pretendía la consagración de la autorización del titular como elemento legitimador para el tratamiento de datos personales. Si bien este elemento no

fue incorporado literalmente en el texto final, se considera incluido por desarrollo de la jurisprudencia constitucional en el núcleo esencial del derecho, mediante la consagración del principio de libertad en el segundo inciso del articulado. En quinta medida, Remolina resaltó la propuesta de Carlos Lleras, quien consideraba que el tratamiento de datos no debería incluirse en la misma regulación del derecho a la intimidad. Esta propuesta finalmente no llegó al texto constitucional (1994)

Estos debates generaron como resultado la consagración del artículo 15 de la Constitución así:

> *"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*[1].
>
> *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"* (Constitución Politica, 1991)

[1] Subraya fuera de texto.

Como puede advertirse, esta es una norma compleja en el sentido en que dentro de un mismo artículo se consagraron tres derechos a saber*: (i) el derecho a la intimidad personal y familiar, (ii) el derecho al buen nombre y (iii) el derecho a la protección de datos personales.*

La evolución de este nuevo derecho fundamental: la protección de datos personales, será analizada a continuación, teniendo en cuenta que esta garantía primero fue consagrada constitucionalmente y su alcance fue descrito a través de principios formulados por la recién creada jurisprudencia constitucional, a diferencia de los derechos a la intimidad y al buen nombre, cuyo contenido y alcance ya llevaban varias décadas.

2.2 Desarrollo jurisprudencial

Habiéndose incluido en la Constitución Política de Colombia una disposición que regula en específico el tratamiento de información en bases de datos desde 1991, surgió el debate sobre cuál era el mecanismo idóneo para que los ciudadanos pudiesen solicitar la efectividad de este derecho, así como la definición de que instancia sería la competente para declarar violaciones o decretar medidas que impidan estas violaciones. Ante la falta de desarrollo legislativo de esta garantía constitucional, la respuesta se encontró en el artículo 86, esto es, la misma norma que consagra la acción de tutela (conocida en otros países como acción de amparo) que le permite a cualquier ciudadano sin necesidad de abogado o formalismos poder solicitar de forma expedita la protección de derechos fundamentales, entre ellos de sus datos personales ante un juez de la República.

Esta acción fue reglamentada mediante el Decreto Ley 2591 de 1991. En esta normativa se describe que una vez haya quedado en firme la decisión de primera instancia, o cuando se encuentre en firme la segunda, todos los expedientes de las acciones de tutela deben ser remitidos a la Corte Constitucional para una eventual revisión, teniendo en cuenta que es el

máximo tribunal constitucional, el cual puede elegir las decisiones a revisar, sin necesidad de motivación expresa y de forma discrecional.

Fue en virtud de esta eventual revisión que la Corte Constitucional profirió su primera sentencia de revisión de tutela en materia de protección de datos personales, conocida en otras latitudes como habeas data, la sentencia T- 414 de 1992. En dicha decisión, la Corte Constitucional aborda la lucha de un ciudadano durante cuatro años, por la corrección de su información de la lista de morosos de la Central de Información de la Asociación Bancaria de Colombia ante una obligación declarada judicialmente extinta por prescripción.

Al analizar el requisito de subsidiariedad como requisito de procedibilidad de la acción de tutela, encontró que los Bancos de Datos, aun cuando algunos recibían información de las entidades vigiladas por la entonces Superintendencia Bancaria, no se encuentran bajo la vigilancia y supervisión de ningún ente de control. (Sentencia T 414, 1992) En esta sentencia puede percibirse la vinculación entre el derecho a la intimidad y el derecho al habeas data, en los siguientes términos:

> *Se protege la intimidad como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad. Esta particular naturaleza suya determina que la intimidad sea también un derecho general, absoluto, extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer "erga omnes", tanto frente al Estado como a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada.*
> *Esta Sala no vacila en reconocer que la prevalencia del derecho a la intimidad sobre el derecho a la información, es consecuencia necesaria de la consagración de la dignidad humana como principio fundamental y valor esencial, a la vez, del Estado social de derecho en que se ha transformado hoy Colombia, por virtud de lo dispuesto en el artículo primero de la Carta de 1991. (...)*
>
> *El dato es un elemento material susceptible de ser convertido en información cuando se inserta en un modelo que lo relaciona con otros datos y hace posible que dicho dato adquiera sentido. El dato que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, es de su propiedad, en el sentido de que tendría ciertos derechos sobre su uso.*

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

Así pues, aunque durante 20 años este derecho consagrado en la Constitución de 1991 no tuvo desarrollo legislativo, fue exigible a través de los mecanismos constitucionales establecidos en el artículo 23, el Derecho de Petición, y el artículo 86, la Acción de Tutela, así como por el numeral 6 del artículo 42 en el Decreto 2591 de 1991, que reglamenta el ejercicio de la acción de tutela[2]. En este orden de ideas, el derecho al habeas data tuvo un amplio desarrollo jurisprudencial, con sentencias como la T-161 de 1993, y la C-913 de 2010, que sirvieron de base para dotar de contenido a las leyes estatutarias 1266, relativa al habeas data financiero, y 1581, de habeas data en general, así como a los decretos que las reglamentan.

En la fase inicial de la jurisprudencia de la Corte Constitucional se evidencia la vinculación del derecho al habeas data con el derecho a la intimidad, como fue expresado en la sentencia C-748 de 2011, así:

> "*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."* (Sentencia C-748, 2011)

A la vez, se emitieron sentencias como la T-340 de 1993 *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*

[2] *Cuando la entidad privada sea aquella contra quien se hubiere hecho la solicitud en ejercicio del hábeas [data], de conformidad con lo establecido en el artículo 15 de la Constitución.* (Decreto 2591, 1991)

jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad" (Sentencia C-748, 2011)

Sin embargo, la línea interpretativa que predominó fue aquella *que apuntó al habeas data como un derecho autónomo. Así, según la Sentencia SU-082 de 1995, el núcleo del derecho al habeas data está compuesto por la autodeterminación informática y la libertad –incluida la libertad económica.* (Sentencia C-748, 2011)

Después, en la Sentencia T-552 de 1997, la Corte Constitucional consagró: "*El derecho al habeas data es, entonces, un derecho claramente diferenciado del derecho a la intimidad, cuyo núcleo esencial está integrado por el derecho a la autodeterminación informativa que implica, como lo reconoce el artículo 15 de la Carta Fundamental, la facultad que tienen todas las personas de "conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas*."

Así mismo, en la Sentencia T-414 de 1992 la Corte delimitó el objeto de protección del habeas data, conforme a la definición dada por el profesor Ernesto Lleras así: "*El dato que constituye un elemento de la identidad de la persona, que en conjunto con otros datos sirve para identificarla a ella y solo a ella, y por lo tanto sería susceptible de usarse para coartarla, es de su propiedad, en el sentido de que tendría ciertos derechos sobre su uso. Datos de este tipo serían sus señales particulares, relaciones de propiedad y de familia, aspectos de su personalidad, y señales de identidad de diversa índole que van emergiendo en las actividades de la vida. Todos estos datos combinados en un modelo, son equivalentes a una "huella digital" porque el individuo es identificable a través de ellos*."

Finalmente, la Corte Constitucional en la Sentencia C-748 del 2011, que analizó la constitucionalidad de la Ley Estatutaria de Protección de Datos Personales, esto es, la Ley 1581 de 2011, reconoció:

> **“***Estos preceptos leídos en conjunto con la primera parte del mismo artículo 15 –sobre el derecho a la intimidad, el artículo 16 –que reconoce el derecho al libre desarrollo de la personalidad- y el artículo 20 –sobre el derecho a la información activo y pasivo y el derecho a la rectificación- de la Carta, han dado lugar al reconocimiento de un derecho fundamental autónomo catalogado como derecho al habeas data, y en algunas oportunidades, como derecho a la* autodeterminación informativa o informática.”

A partir de la exposición anterior, puede decirse entonces que el principal legado de la Corte Constitucional en relación con la protección de datos personales fue la definición de los principios que permitieron establecer si la actividad de tratamiento se está ejecutando en debida forma, con ocasión a la revisión de las sentencias de tutela. En ellas, en mayor medida el conflicto giró en torno a datos de carácter financiero y crediticio, principios que posteriormente fueron recogidos por el legislador en las leyes estatutarias 1266 y 1581.

Remolina (Tratamiento de Datos Personales. aproximación internacional y comentarios a la Ley 1581 de 2012, 2013), explica que estos principios de origen jurisprudencial y el orden en que serán presentados, obedece a que los primeros ocho fueron ratificados en la Ley Estatutaria 1266, mientras que los siguientes tres fueron positivizados en la ley 1581, la cual también consagra los primeros. Aquí es importante resaltar que el derecho al habeas data es difícil de regular, conforme metodologías tradicionales propias del derecho de propiedad. Por ello, es un derecho que ha sido desarrollado mediante la aplicación de principios que de forma flexible delimitan su contenido. En este orden de ideas, a continuación, serán presentados los principios desarrollados por las leyes estatutarias de origen jurisprudencial.

2.2.1 Veracidad o calidad de los registros o datos

Para que puedan cumplir con el objetivo de informar, los datos deben ser veraces y cumplir con mínimos de calidad para la adecuada toma de decisiones y el correcto análisis de la

información. Por ello, este principio se desprende del análisis armónico de los derechos consagrados en los artículos 15 y 20 de la Constitución, relacionados con el derecho a la información. Este último señala: *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.*

En este sentido, en sentencias como la SU-082 de 1995, la Corte Constitucional ha reconocido: "*Hay que partir de la base de que la información debe corresponder a la verdad, ser veraz, pues no existe derecho a divulgar información que no sea cierta*." De ahí que este principio se materialice en un derecho del titular de la información llamado "rectificación", consistente en la prerrogativa para exigir al responsable o encargado del tratamiento de datos la corrección de información cuando esta sea falsa, incorrecta, no susceptible de ser comprobada o incompleta, de tal forma que pueda inducir a terceros en error.

Este mismo principio se materializa con una obligación en cabeza de aquellos que desean manejar datos personales, quienes tiene el deber de garantizar la calidad de la información. Esta garantía implica medidas técnicas y jurídicas tales como la inclusión de sistemas de validación de la información para detectar casos como duplicidades o contradicciones en una base de datos, así como la posibilidad de contrarrestar o validar la información con otra base de datos.

De cara a las medidas jurídicas se encuentra la obligación de corrección inmediata de la información, o de forma más específica los principios de integralidad e incorporación. El primero, en relación con la completitud como atributo de la información que repose sobre un individuo y, el segundo, cómo la facultad que tiene el titular de solicitar que se añada información veraz que permita dar una verdadera apreciación de su identidad. Así las cosas, queda prohibido al poseedor de una base de datos la negativa a modificar o añadir información que cumpla con estos principios de forma injustificada.

Para entender mejor este último supuesto, es pertinente traer a colación el caso de la Sentencia T-303 de 1998, donde al analizar una acción de tutela en la que el accionante pretendía la eliminación de un dato negativo (mora), la Corte Constitucional establece: "[…]*sin desconocer el derecho a la información de las centrales y archivos de datos y de las instituciones financieras —indispensable para un adecuado funcionamiento del sistema crediticio—, reivindica el que toda persona tiene a verificar qué se difunde acerca de ella y cuál es el fundamento de los datos correspondientes, así como a corregir o aclarar lo inexacto y solicitar la eliminación de las informaciones falsas o erróneas que, por tanto, lesionan su buen nombre, y las de aquellas que invaden la órbita reservada de su intimidad personal o familiar.*[…]"

En ese sentido señala: "*Es evidente que la permanencia del dato negativo equivocado causa, minuto a minuto, enorme daño a la persona, por lo cual es indudablemente contraria a la Constitución y altamente ofensiva para la dignidad del individuo, y que si, habiendo sido reclamada directamente la rectificación en ejercicio del Habeas Data, ella no se produce inmediatamente, hay lugar al ejercicio de la acción de tutela contra la entidad para obtener la protección del derecho fundamental violado, por medio de una orden judicial perentoria."*

No obstante, en este fallo se da claridad sobre la no procedencia de la rectificación, toda vez que el accionante si incurrió en mora en la obligación y, por lo tanto, lo procedente es la actualización e integración de la información sobre su estado actual, es decir, que sí estuvo en mora, pero actualmente ya no lo está. El derecho de actualización será abordado al analizar el principio de temporalidad del dato.

2.2.2 Finalidad

Este principio es la materialización del elemento de la existencia de las obligaciones "causa lícita"[3]. En materia de habeas data, implica que el tratamiento de datos debe responder a una finalidad legitima en los términos de la constitución y la ley, quedando proscrito, por ejemplo, el tratamiento de datos cuyo fin sea discriminar negativamente en violación del derecho a la igualdad o la ejecución de un delito. En ese sentido, cada dato que se recopile en ejercicio del tratamiento de datos debe responder directamente a la finalidad del tratamiento, prohibiéndose en consecuencia la recopilación de información que sea considerada impertinente para la finalidad, ejemplo de ello sería preguntar la afinidad política en una historia clínica.

Adicionalmente esta finalidad es uno de los elementos que permiten al juez o a la entidad de vigilancia y control, establecer si quien recolecta los datos está realizando un adecuado tratamiento de estos, conforme a las finalidades previamente establecidas, pues determinará medidas como: (i) la existencia o no de medidas de circulación restringida, y (ii) si el uso de la base de datos se está realizando para la finalidad que se creó. De esta forma, la primera medida consistirá en la obligación de informar al titular sobre la finalidad del tratamiento de datos y la posibilidad de pedir la eliminación de sus datos en caso de que a estos se les use con un fin diferente al informado.

Al respecto, Remolina (2013) señala que la Corte Constitucional al revisar si el acceso público a las bases de datos de Catastro y del Instituto Nacional de Salud atentaba o no contra la intimidad de los ciudadanos, estableció: "[…] *tanto el acopio, el procesamiento y la*

[3] Artículo 1524 Código Civil colombiano: *CAUSA DE LAS OBLIGACIONES. No puede haber obligación sin una causa real y lícita; pero no es necesario expresarla. La pura liberalidad o beneficencia es causa suficiente. Se entiende por causa el motivo que induce al acto o contrato; y por causa ilícita la prohibida por la ley, o contraria a las buenas costumbres o al orden público.*

divulgación de los datos personales, debe obedecer a una finalidad constitucionalmente legítima, definida de manera clara, suficiente y previa; de tal forma que queda prohibida la recopilación de datos sin la clara especificación acerca de la finalidad de los mismos, así como el uso o divulgación de datos para una finalidad diferente a la inicialmente prevista". (Sentencia T-729, 2002)

En el caso de las centrales de riesgo, por ejemplo, la Corte Constitucional ha descrito la finalidad de este tratamiento de datos así:

> "*Las instituciones de crédito, precisamente por manejar el ahorro del público, ejercen una actividad de interés general, como expresamente lo señala el artículo 335 de la Constitución. No tendría sentido pretender que prestaran sus servicios, y en particular otorgaran créditos, a personas de las cuales no tienen información. Por el contrario: un manejo prudente exige obtener la información que permita prever qué suerte correrán los dineros dados en préstamo.*
>
> *Obsérvese que cuando un establecimiento de crédito solicita información sobre un posible deudor, no lo hace por capricho, no ejerce innecesariamente su derecho a recibir información. No, la causa de la solicitud es la defensa de los intereses de la institución que, en últimas, son los de una gran cantidad de personas que le han confiado sus dineros en virtud de diversos contratos*" (Sentencia SU-082, 1995)

De esa manera se puede establecer que, si la central de riesgos recopila datos como la orientación sexual del titular, este dato se trataría en violación del principio de finalidad, dado que nada tiene que ver con el riesgo crediticio del titular.

2.2.3 Circulación restringida

Este principio es el que permite diferenciar el alcance del derecho a la intimidad del derecho a la protección de datos personales. En materia de habeas data se hace necesaria la clasificación

de los datos, pues no todos tienen las mismas características. En la Sentencia SU-082 de 1995 la Corte Constitucional usa un listado del autor Eduardo Novoa Monreal para ejemplificar los datos privados, es decir aquellos que se encuentran bajo el ámbito de protección del derecho a la intimidad, como son:

> "*a] ideas y creencias religiosas, filosóficas, mágicas y políticas que el individuo desee sustraer del conocimiento ajeno;*
>
> *"b] aspectos concernientes a la vida amorosa y sexual;*
>
> *"c] aspectos no conocidos por extraños de la vida familiar, especialmente los de índole embarazosa para el individuo o para el grupo*;"

Estos ejemplos permiten inferir que los datos privados son aquella información que sólo interesa al titular.

Ahora bien, por oposición, los datos públicos son "*datos calificados como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas*" (Ley 1266, 2008)

Esta amplia definición de dato público dada en la Ley 1266 fue moderada posteriormente en la Ley 1712 de 2014, que desarrolla el ejercicio del derecho de acceso a la información, mediante la cual se agregaron dos clasificaciones más: Por un lado, "*la 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 semi-privado 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.* " Por el otro, la información pública reservada, la cual 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." (Ley 1712, 2014)

El derecho a la protección de datos personales reconoce que existe información que interesa al titular, pero que también puede interesar a terceros por circunstancias como las descritas al analizar el principio de finalidad. Estos datos son los datos semiprivados, como sucede con el historial crediticio o la experiencia laboral de un individuo. De conformidad con lo conceptuado por la jurisprudencia de la Corte Constitucional, el principio de circulación restringida nace de la tensión entre el habeas data y el derecho de acceso a la información, estableciendo que el nivel de accesibilidad de la información está directamente relacionado con su clasificación, de la siguiente forma:

> "*Así, la información pública, calificada como tal según los mandatos de la ley o de la Constitución, puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal. Por vía de ejemplo, pueden contarse los actos normativos de carácter general, los documentos públicos en los términos del artículo 74 de la Constitución, y las providencias judiciales debidamente ejecutoriadas; igualmente serán públicos, los datos sobre el estado civil de las personas o sobre la conformación de la familia. Información que puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno.*
>
> *La información semiprivada, será aquella que por versar sobre información personal o impersonal y no estar comprendida por la regla general anterior, presenta para su acceso y conocimiento un grado mínimo de limitación, de tal forma que la misma sólo puede ser obtenida y ofrecida por orden de autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales. Es el caso de los datos relativos a las relaciones con las entidades de*

> *la seguridad social o de los datos relativos al comportamiento financiero de las personas.*
>
> *La información privada, será aquella que por versar sobre información personal o no, y que, por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio.*
>
> *Finalmente, encontramos la información reservada, que por versar igualmente sobre información personal y sobre todo por su estrecha relación con los derechos fundamentales del titular - dignidad, intimidad y libertad- se encuentra reservada a su órbita exclusiva y no puede siquiera ser obtenida ni ofrecida por autoridad judicial en el cumplimiento de sus funciones. Cabría mencionar aquí la información genética, y los llamados "datos sensibles" o relacionados con la ideología, la inclinación sexual, los hábitos de la persona, etc."* (Sentencia T-729, 2002)

Sobre esta última clasificación de datos sensibles es pertinente señalar que la Corte con posterioridad ha reconocido que es posible el tratamiento de datos sensibles; no obstante al considerarse reservada o estrechamente ligada con la intimidad de las personas, el tratamiento debe hacerse bajo un control más riguroso, y en concordancia con el principio de finalidad, es decir, es preciso establecer para qué se necesitan y se van a usar esos datos, así como implementar mayores medidas técnicas y jurídicas que garanticen la seguridad y circulación restringida de esta información. En otras palabras, se busca que sólo accedan a ella los funcionarios que se encuentren legitimados por la Constitución, la ley o el ejercicio de sus funciones.

En consecuencia, el principio de circulación restringida también representa para la persona o entidad que hace tratamiento datos la obligación de implementar medidas técnicas como:

cifrado, bloqueo por usuarios, sistema de información más robustos que impidan el fácil acceso a datos personales de personas sin autorización; así como medidas jurídicas tales como compromisos contractuales, cláusulas de confidencialidad, garantías, etc.

Posteriormente, la Ley 1266 consagró expresamente: "*Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley*". Esto resulta coherente con lo afirmado por la Corte Constitucional en la Sentencia T-729 del 2002, donde expresó: "[Catastro] *al facilitar el acceso a información personal de manera indiscriminada, distorsiona la finalidad a la cual estaba llamada la base de datos, pues permite que extraños, sin intereses visibles, accedan a la información sin que sea posible ningún tipo de control por parte de sus titulares*."

2.2.4 Temporalidad de la información

La información negativa en determinadas centrales de información puede ocasionar una versión contemporánea de la *capitis deminutio* o muerte civil del Derecho Romano, pues, aunque no lo haga jurídicamente, sí lo hace materialmente. En efecto, quien tiene un antecedente penal o un reporte negativo en su historial crediticio ve automáticamente afectada, disminuida y en algunos casos hasta extinguida, su posibilidad de celebrar contratos como los laborales o con el sector financiero.

Esta realidad fue advertida desde la primera oportunidad en que la Corte Constitucional conceptuó sobre el derecho de habeas data, describiéndola así: "*El encarcelamiento del alma en la sociedad contemporánea, dominada por la imagen, la información y el conocimiento, ha demostrado ser un mecanismo más expedito para el control social que el tradicional encarcelamiento del cuerpo. […]*

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

De otra parte, es bien sabido que las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia después de algún tiempo tales personas son titulares de un verdadero derecho al olvido." (Sentencia T-414, 1992) Cobra vigencia aquí el derecho a la actualización de la información, el cual implica una prerrogativa en favor del titular de la información, para que se señale la vigencia de la información negativa, y si dicha falta o incumplimiento ha sido subsanado, esto también sea informado.

Adicionalmente, la Corte Constitucional desarrolló el derecho al olvido o "caducidad del dato negativo" bajo el entendido que, una vez acaecidas ciertas condiciones, el titular puede exigir la eliminación absoluta de la información negativa al considerase que aún un recuento histórico de esta se convertiría en una pena perpetua. A falta de desarrollo por el legislador, en 1995 la Corte Constitucional creó las primeras reglas de caducidad de la información negativa en materia crediticia:

> "*En este orden de ideas, sería irrazonable la conservación, el uso y la divulgación informática del dato, si no se tuviera en cuenta la ocurrencia de todos los siguientes hechos:*
>
> *a) Un pago voluntario de la obligación;*
>
> *b) Transcurso de un término de dos (2) años, que se considera razonable, término contado a partir del pago voluntario. El término de dos (2) años se explica porque el deudor, al fin y al cabo, pagó voluntariamente, y se le reconoce su cumplimiento, aunque haya sido tardío. Expresamente se exceptúa el caso en que la mora haya sido*

inferior a un (1) año, caso en el cual, el término de caducidad será igual al doble de la misma mora; y,

c) Que durante el término indicado en el literal anterior, no se hayan reportado nuevos incumplimientos del mismo deudor, en relación con otras obligaciones.

Si el pago se ha producido en un proceso ejecutivo, es razonable que el dato, a pesar de ser público, tenga un término de caducidad, que podría ser el de cinco (5) años, que es el mismo fijado para la prescripción de la pena, cuando se trata de delitos que no tienen señalada pena privativa de la libertad, en el Código Penal. Pues, si las penas públicas tienen todas un límite personal, y aun el quebrado, en el derecho privado, puede ser objeto de rehabilitación, no se ve por qué no vaya a tener límite temporal el dato financiero negativo. Ahora, como quiera que no se puede perder de vista la finalidad legítima a la que sirven los bancos de datos financieros, es importante precisar que el límite temporal mencionado no puede aplicarse razonablemente si dentro del mismo término ingresan otros datos de incumplimiento y mora de las obligaciones del mismo deudor o si está en curso un proceso judicial enderezado a su cobro.

Esta última condición se explica fácilmente pues el simple pago de la obligación no puede implicar la caducidad del dato financiero, por estas razones: la primera, la finalidad legítima del banco de datos que es la de informar verazmente sobre el perfil de riesgo de los usuarios del sistema financiero; la segunda, la ausencia de nuevos datos negativos durante dicho término, que permite presumir una rehabilitación comercial del deudor moroso. Es claro que si durante los cinco (5) años mencionados se presentan nuevos incumplimientos de otras obligaciones, se pierde la justificación para excluir el dato negativo. ¿Por qué? Sencillamente porque en este caso no se ha reconstruido el buen nombre comercial.

> *Sin embargo, cuando el pago se ha producido una vez presentada la demanda, con la sola notificación del mandamiento de pago, el término de caducidad será solamente de dos (2) años, es decir, se seguirá la regla general del pago voluntario.*
>
> *Igualmente debe advertirse que, si el demandado en proceso ejecutivo invoca excepciones, y éstas prosperan, y la obligación se extingue porque así lo decide la sentencia, el dato que posea el banco de datos al respecto, debe desaparecer. Naturalmente se exceptúa el caso en que la excepción que prospere sea la de prescripción, pues si la obligación se ha extinguido por prescripción, no ha habido pago, y, además, el dato es público*." (Sentencia SU-082, 1995)

Actualmente, esta regla se encuentra fijada en la Ley 1266 y es conocida por la doctrina como la regla del tope, estableciendo que: *Los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera, y en general, aquellos datos referentes a una situación de incumplimiento de obligaciones, se regirán por un término máximo de permanencia, vencido el cual deberá ser retirada de los bancos de datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información. El término de permanencia de esta información será de cuatro (4) años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea pagada la obligación vencida*. (Ley 1266, 2008)

No obstante, en el análisis de constitucionalidad de esta ley estatuaria, la Corte califica como desproporcional la imposición de un mismo término de caducidad sin consideración a las posibles circunstancias de incumplimiento, por lo cual fijó como condición para declarar "*la exequibilidad que (i) se aplique el término razonable desarrollado por la jurisprudencia constitucional antes analizada, equivalente al duplo de la mora, respecto de las obligaciones que permanecieron en mora durante un plazo corto; y (ii) extienda el plazo de permanencia previsto por el legislador estatutario a los eventos en que se predice la extinción de la obligación en mora."* (Sentencia C-1011, 2008) Esta segunda regla es conocida como el doble

y para poder entenderla en relación con la regla del tope, es necesario diferenciar los dos tipos de reportes negativos, donde el primero es aquel reporte que indica la mora actual y el tiempo de esa mora; mientras que el segundo, bautizado por la doctrina como "reporte sanción", es aquel que señala que ese deudor estuvo, pero ya no está en mora.

Estas condiciones de exequibilidad afectaron ambos tipos de reporte. En primera medida, el reporte negativo estará vigente, siempre y cuando la obligación también lo esté; esto implica que si la obligación se extingue por cualquiera de los modos que establece el Código Civil[4], el reporte negativo también deberá dar cuenta de esta situación. En segunda medida, una vez extinta la obligación empieza a contarse el término de caducidad del "reporte sanción", el cual debe ser igual al doble del tiempo que el deudor estuvo en mora hasta la extinción de la obligación, sin superar un término mayor a cuatro años de reporte sanción.

Por esta modificación existe la percepción de que la Ley 1266 extendió el término de prescripción extraordinaria de las obligaciones de 10 a 14 años. No obstante, esta percepción es errada, pues durante la vigencia del reporte sanción la obligación ya no es exigible judicialmente. Cabe señalar que, dependiendo de la información financiera, los encargados de tratamiento de datos, en su mayoría, centrales de riesgo, deben emitir un puntaje o una calificación al titular de los datos, calificación que puede significar el otorgamiento o no de un producto financiero, en caso de ser un puntaje bajo, o el acceso a condiciones más favorables en tasas de interés cuando el puntaje es alto. Este puntaje no varía cuando culmina el término del reporte sanción, de forma que si bien es cierto ya no se registra que el titular alguna vez estuvo en mora, no está previsto que este derecho al olvido se materialice en el puntaje que le

[4] Artículo 1625. Modos De Extinción. Toda obligación puede extinguirse por una convención en que las partes interesadas, siendo capaces de disponer libremente de lo suyo, consientan en darla por nula. Las obligaciones se extinguen además en todo o en parte: 1o.) Por la solución o pago efectivo. 2o.) Por la novación. 3o.) Por la transacción. 4o.) Por la remisión. 5o.) Por la compensación. 6o.) Por la confusión. 7o.) Por la pérdida de la cosa que se debe. 8o.) Por la declaración de nulidad o por la rescisión. 9o.) Por el evento de la condición resolutoria. 10.) Por la prescripción

es otorgado, por lo que el reporte negativo aun cuando desaparece sigue teniendo efectos adversos para titular.

Ahora bien, en materia de antecedentes penales, actualmente no existe ley, por lo que se encuentra regulado por lo dispuesto en las leyes 1581 y 1712, ya descritas con anterioridad. Sin embargo, es importante resaltar la Sentencia SU-458 de 2012, que en materia de temporalidad de este dato negativo establece:

> "*En una primera faceta es posible ejercer la facultad de supresión con el objeto de hacer desaparecer por completo de la base de datos, la información personal respectiva. Caso en el cual la información debe ser suprimida completamente y será imposible mantenerla o circularla, ni siquiera de forma restringida (esta es la idea original del llamado derecho al olvido). En una segunda faceta, la facultad de supresión puede ser ejercitada con el objeto de hacer desaparecer la información que está sometida a circulación. Caso en el cual la información se suprime solo parcialmente, lo que implica todavía la posibilidad de almacenarla y de circularla, pero de forma especialmente restringida.*
>
> *Esta segunda modalidad de supresión es una alternativa para conciliar varios elementos normativos que concurren en el caso de la administración de información personal sobre antecedentes penales. Por un lado, la supresión total de los antecedentes penales es imposible constitucional y legalmente. Ya lo vimos al referir el caso de las inhabilidades intemporales de carácter constitucional, las especiales funciones que en materia penal cumple la administración de esta información personal, así como sus usos legítimos en materia de inteligencia, ejecución de la ley y control migratorio. En estos casos, la finalidad de la administración de esta información es constitucional y su uso, para esas específicas finalidades, está protegido además por el propio régimen del habeas data. Sin embargo, cuando la administración de la*

> *información personal relacionada con antecedentes pierde conexión con tales finalidades deja de ser necesaria para la cumplida ejecución de las mismas, y no reporta una clara utilidad constitucional; por tanto, el interés protegido en su administración pierde vigor frente al interés del titular de tal información personal. En tales casos, la circulación indiscriminada de la información, desligada de fines constitucionales precisos, con el agravante de consistir en información negativa, y con el potencial que detenta para engendrar discriminación y limitaciones no orgánicas a las libertades, habilita al sujeto concernido para que en ejercicio de su derecho al habeas data solicite la supresión relativa de la misma*". (Sentencia SU-458, 2012)

En consecuencia, quien tenga una pena prescrita o cumplida tiene derecho a la supresión relativa del dato sin perjuicio de que terceros que acrediten una finalidad legitima[5] puedan pedir una verificación completa de antecedentes ante el administrador de la base de datos, quien actualmente es la Policía Nacional. Cabe resaltar que esta verificación requiere la autorización del titular de la información.

2.2.5 Interpretación integral de derechos constitucionales

Tal y como lo demuestran las sentencias citadas previamente, el derecho de habeas data suele tener tensiones con otros derechos de igual relevancia constitucional, como son la intimidad, el acceso a la información e, incluso, con el derecho a la vida y a la dignidad humana, como es el caso de la información médica o de los antecedentes penales. Por ello, el principio de interpretación integral de derechos constitucionales ratifica la posibilidad de ponderar los

[5] Ejemplo de ello un colegio estaría legitimado para hacer esta revisión en el caso de la contratación de sus docentes o personal en virtud de la prevalencia de los derechos de los niños consagrada en el artículo 44 de la Constitución Política.

derechos en conflicto cuando se encuentren en tensión, de manera que su prelación o relativización dependerá de cada caso concreto.

2.2.6 Seguridad

Este principio es resultado de la aplicación de los principios de calidad y circulación restringida, implicando la obligación de tener "*las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado*". (Ley 1266, 2008) para introducir este principio, la Corte Constitucional desde la Sentencia T-414 de 1992, hace un reconocimiento de la asimetría en la relación entre el ciudadano y quienes ostentan el poder derivado del uso que hacen de la información del ciudadano, asimetría bautizada como "poder informático".

El ejercicio de esta potestad informática, lleva a recordar a Franklin D. Roosevelt quien en 1945 afirmó: "*great power involves great responsibility*"; para este caso la gran responsabilidad implica la inversión en sistemas técnicos, que materialmente impidan el deterioro de la información, así como también en programas de gestión documental, como los descritos en la Ley 594 del 2000, para las entidades públicas. De esta forma, la implementación de medidas de seguridad debe ser coherente con el desarrollo tecnológico actual.

De ahí que tanto la jurisprudencia como el legislador acudan al principio de neutralidad tecnológica, el cual evita que los requerimientos jurídicos en materia de seguridad sean asociados a la implementación de una tecnología específica, dejando al arbitrio del responsable y del encargado del tratamiento de datos la elección de las medidas a implementar según los canales de recolección, almacenamiento y eliminación de la información a su cargo.

2.2.7 Confidencialidad

Este principio es una ampliación del espectro del principio de circulación restringida, el cual está dirigido a quienes administran los datos y que están obligados a cumplir con el principio de seguridad anteriormente descrito. No obstante, se debe resaltar que el principio de confidencialidad aquí se extiende la obligación de mantener en reserva los datos personales que se conozcan, aún con posterioridad a la terminación del vínculo contractual, por el cual se tuvo acceso a la base de datos.

De manera que la obligación de confidencialidad no requiere de su estipulación contractual, pues tiene un origen jurisprudencial, y actualmente legal, el cual sólo pudo tener consecuencias jurídicas con la expedición del régimen sancionatorio en materia de protección de datos personales bajo las leyes 1266, 1273 y 1581, a las cuales se hará referencia con posterioridad.

2.2.8 Libertad

Este es el principio más importante en materia de datos personales. Este postulado dio origen a la definición de titular del dato personal, como aquella persona natural o jurídica sobre quien los datos se refieren, prevista desde Constitución de 1991.

Esta libertad fue definida por la Corte Constitucional como "*la facultad de disponer de la información, de preservar la propia identidad informática, es decir, de permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás.*" (Sentencia T-414, 1992)

La Corte advirtió desde entonces que a esta facultad de disposición […] *frente al dato no puede aplicarse en todo su rigor el derecho clásico de propiedad. En verdad, bien miradas las cosas, salta a la vista la existencia de varios sujetos con distintas relaciones. Uno es el sujeto del cual se dice algo o al cual algo le concierne en el universo informativo construido a partir del dato.* [Titular del dato] *Otro es el sujeto que, aplicando unos códigos o gramáticas como*

instrumentos auxiliares, hace que el dato se convierta en información. [Fuente del dato] *Pueden existir otros cuya labor específica es la circulación y difusión de la información con destino a los clientes habituales de los medios de comunicación* [Encargado del tratamiento]. *La labor primordial de estos últimos sujetos es, como se ve, hacer que el dato se convierta en esa mercancía denominada a veces noticia, apta para el consumo de su clientela que las nuevas tecnologías de información permiten ampliar más y más cada día. En estas condiciones, los diversos sujetos son apenas titulares de algunas facultades que no les confieren necesariamente la calidad de propietarios. Muchas veces no son más que simples depositarios forzosos*" (Sentencia T-414, 1992)

Así las cosas, dada la redacción del artículo 15 en la Constitución Política, para la Corte Constitucional ha sido aceptado que el principio de libertad da lugar a una regla general "*La autorización del titular es un requisito indispensable para el tratamiento de datos personales*" (Sentencia SU-082, 1995). Sin embargo, esta autorización debe cumplir con ciertos requisitos para su validez: debe ser libre, previa y expresa.

En relación con la calidad de libre, la jurisprudencia ha señalado que la autorización para tratamiento de datos no puede ser producto de presiones o constreñimientos en contra del titular. En la práctica esto no es tan cierto, toda vez que la autorización para el tratamiento de datos se ha convertido en un requisito para la celebración de contratos como la prestación de servicios financieros o de telecomunicaciones.

En lo que respecta a la oportunidad en la que debe ser otorgada, desde 1992 la Corte Constitucional ha señalado que el tratamiento de datos sólo puede ser considerado lícito si se hace con autorización del titular. Cabe señalar que las consecuencias de no contar con esta autorización recaen directamente sobre la validez de eventuales reportes, en particular los negativos, donde el principio de calidad de la información cede en favor del principio de libertad; ello implica que sin importar la veracidad y completitud del reporte hecho, si este se

hizo en virtud del tratamiento de datos sin autorización el reporte deberá removerse como si jamás hubiese existido. (Sentencia T-964, 2010)

Por último, la autorización no se presume ni puede ser producto del silencio o de la inactividad del titular. Sin embargo, la jurisprudencia constitucional reconoció que existen excepciones al requisito de contar con la autorización del titular de la información: cuando el tratamiento es en virtud de una orden legal o, si se da en ejercicio de funciones judiciales.

Ambas excepciones se dan en virtud de la materialización del principio de finalidad del tratamiento de datos, que reconoce que el manejo de información personal puede ejercerse para satisfacer intereses superiores que la voluntad del titular de la información. Ejemplo de ello: el tratamiento en bajo el ejercicio de funciones judiciales responde directamente a la finalidad de administrar justicia. Absurdo sería que un investigado o un imputado puede solicitar la exclusión, eliminación o prohibir el tratamiento de sus datos personales. De ahí que la Sentencia SU-458 del 2012 defina que procede solo la "supresión relativa" de la información.

2.2.9 Transparencia

Tal y como el artículo 15 de la Constitución dispone: *Todas las personas 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*. El principio de transparencia, pues, gira en torno al primer verbo rector: conocer.

En materia de habeas data, no es concebible que al titular de la información se le responda que la información sobre sí mismo es confidencial. De igual forma, el cumplimiento de este principio conlleva la necesidad de implementar procedimientos ágiles y sencillos para que el titular pueda acceder a su propia información. Este es uno de los escenarios donde con frecuencia se acude al derecho fundamental de petición.

Además de conocer sus propios datos personales, el principio de transparencia demanda para las empresas y personas que hacen tratamiento de datos la obligación de emitir y poner a disposición de los titulares políticas de privacidad, donde pueda accederse directamente a los usos y tratamientos que se están dando, de forma que el titular tenga las herramientas necesarias para ejercer su derecho de autorización en cualquier momento ya sea modulándolo. Es decir, admitir o no ciertos usos o revocándolo.

2.3 Desarrollo legislativo

Como pudo constatarse en la sección anterior, el desarrollo jurisprudencial del contenido del derecho de protección de datos personales en materia financiera. Si bien estos precedentes jurisprudenciales representaron importantes conquistas para los titulares de datos, carecían de términos o procedimientos claros para el ejercicio de este derecho distintos a la acción de tutela, y de un régimen sancionatorio en caso de incumplimiento. Así las cosas, 16 años después de proferida la Sentencia T-414 de 1992, el Congreso de la República de Colombia, en ejercicio de lo dispuesto en el artículo 152[6] de la Constitución Política, positivizó mediante leyes estatutarias las garantías expuestas por la Corte Constitucional que serán abordadas según el orden cronológico de su expedición: la ley sectorial, 1266 de 2008, la Ley General de Protección de Datos Personales, 1581 del 2011, y la Ley Estatutaria de Acceso a la Información Pública, 1712 de 2014.

2.3.1 Ley Sectorial de Protección de Datos: Ley 1266 de 2008

En la exposición de motivos publicada, junto con el proyecto de ley estatutaria, en la Gaceta del Congreso 243 del 25 de julio de 2006 se ratifican las afirmaciones del juez constitucional

[6] "*ARTICULO 152. Mediante las leyes estatutarias, el Congreso de la República regulará las siguientes materias: a) Derechos y deberes fundamentales de las personas y los procedimientos y recursos para su protección; b) Administración de justicia; c) Organización y régimen de los partidos y movimientos políticos; estatuto de la oposición y funciones electorales; d) Instituciones y mecanismos de participación ciudadana. e) Estados de excepción. f) La igualdad electoral entre los candidatos a la Presidencia de la República que reúnan los requisitos que determine la ley".* (Constitución Politica, 1991)

sobre la existencia de una laguna normativa que, a la fecha de dicho proyecto, afectaba a 1.3 millones de colombianos, cuyos datos ya eran tratados por centrales de riesgo, información que no se restringía al comportamiento en el sector financiero, sino que empezaba a ampliarse a otros sectores como colegios, donde la respuesta del ordenamiento jurídico se restringía a fallos de revisión de acciones de tutela que inicialmente tiene efectos interpartes (Proyecto de ley estatutaria número 27, 2006, pág. 15).

Así pues, inicialmente la Ley 1266 en materia de información financiera[7] designa las autoridades encargadas de la supervisión, vigilancia y control sobre las entidades que hacen tratamiento de datos personales: La Superintendencia de Industria y Comercio, de forma general, y la Superintendencia Financiera de Colombia, sólo para las entidades que ya se encontraban bajo su vigilancia. Asimismo describe el procedimiento especial que se surtirá en sus delegaturas en caso de incumplimiento de los deberes y derechos consagrados en la norma, el cual se rige de manera subsidiaria por las normas del procedimiento administrativo sancionatorio fijando de manera expresa sanciones que van desde multas a título personal e institucional, que pueden ascender hasta los 1.500 salarios mínimos mensuales vigentes, suspensión, o incluso, prohibición de realizar actividades de tratamiento de datos.

En virtud del principio de finalidad, esta ley reconoce como principal objeto del tratamiento de datos personales en materia financiera el "favorecer los fines de expansión y democratización del crédito". En ese sentido, fija como sancionable la negativa en otorgamientos de productos financieros sustentada exclusivamente en la existencia de un dato negativo.

[7] Al respecto la delimitación del objeto de esta Ley está dada por la definición del artículo tercero como: inf*ormaci*ón financiera, *crediticia, comercial, de servicios y la proveniente de terceros países, aquella referida al nacimiento, ejecución y extinción de obligaciones dinerarias, independientemente de la naturaleza del contrato que les dé origen*. (Ley 1266, 2008)

Esta norma mantiene la definición de dato personal data en la Sentencia T-414 de 1992. Sin embargo, incorpora la definición y diferenciación entre fuente, operador y usuario a tratamiento de datos en su artículo 3 así:

"*b) Fuente de información. Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, en razón de autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar la protección de los derechos del titular de los datos;*

c) Operador de información. Se denomina operador de información a la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la presente ley. Por tanto el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente;" (Ley 1266, 2008)

Dado que las leyes objeto de revisión en este documento son estatutarias, su análisis implica una remisión directa a las sentencias que analizaron su constitucionalidad. En efecto, este

análisis se dio de forma previa, automática y completa, de acuerdo con lo previsto en el procedimiento legislativo descrito el artículo 153 de la Constitución[8].

En el caso de la Ley 1266, su análisis en conjunto con la Sentencia C-1011 de 2008 cobra relevancia, dado que el análisis de la Corte Constitucional incluyo importantes modificaciones al proyecto de ley, como fue presentado, entre las que se incluye la extensión de la aplicación de la normativa a las entidades de carácter público cuando éstas acceden a información de operadores de la información y la inclusión de las reglas del doble y del tope correspondientes el principio de temporalidad del dato negativo formuladas en la Sentencia SU-082 de 1995, principalmente.

Por primera vez, a escala legislativa se fijan las condiciones para el tratamiento de datos con encargados y/o responsables que no estén ubicados en el territorio nacional, imponiendo como requisitos para poder hacer tratamiento de datos de colombianos:

a) La constitución como persona jurídica en Colombia.
b) La habilitación de un punto de atención a titulares de la información.
c) La actualización de la información que reporten las fuentes cada 10 días.
d) La implementación de herramientas tecnológicas y jurídicas que garanticen la seguridad e integridad de la información (Ley 1266, 2008).

Esta ley mantiene las clasificaciones de datos en privado, semiprivado y público que fueron formulados en la Sentencia SU-082 del 1995, circunscribiendo el ámbito de aplicación de la norma, es decir los datos financieros y comerciales como semiprivados. Lo anterior implica que los datos financieros y comerciales "*no tiene naturaleza íntima, reservada, ni pública y*

[8] *ARTÍCULO 153. La aprobación, modificación o derogación de las leyes estatutarias exigirá la mayoría absoluta de los miembros del Congreso y deberá efectuarse dentro de una sola legislatura.*
Dicho trámite comprenderá la revisión previa, por parte de la Corte Constitucional, de la exequibilidad del proyecto. Cualquier ciudadano podrá intervenir para defenderla o impugnarla. (Constitución Politica, 1991)

cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general" (Ley 1266, 2008)

2.3.2 Ley General de Protección de Datos Personales: Ley 1581 de 2011

Posteriormente, en 2011 se expidió la norma general en materia de protección de datos personales. Este ordenamiento suple de forma subsidiaria lo no regulado por la Ley 1266 y regulando bases de datos que se escaparon al control de la ley sectorial, entre ellas las bases de datos con información comercial, mercadeo, médica, académica, administrativa, etc.

En lo que concierne a la Ley 1581, fue la Sentencia C-748 de 2011 la que contuvo su análisis de constitucionalidad dentro del control previo que requieren las leyes estatutarias. En el referido fallo, la Corte Constitucional advirtió que la definición de dato personal limitaba el ámbito de aplicación de la norma, pues aparentemente excluía los datos de persona jurídicas. Al respeto señaló:

"Sin embargo, en sentir de la Sala, no se trata de una restricción que desconozca la doctrina constitucional sobre la protección del habeas data en cabeza de las personas jurídicas, ni el principio de igualdad. Ciertamente, la garantía del habeas data a las personas jurídicas no es una protección autónoma a dichos entes, sino una protección que surge en virtud de las personas naturales que las conforman. Por tanto, a juicio de la Sala, es legítima la referencia a las personas naturales, lo que no obsta para que, eventualmente, la protección se extienda a las personas jurídicas cuando se afecten los derechos de las personas que la conforma" (Sentencia C-748, 2011)

Lo anterior, contrario a lo dispuesto en la Ley 1266, cuyos efectos sí están expresamente extendidos a datos de personas jurídicas y naturales. A diferencia de la precitada ley, que incorpora la definición de fuente, usuario y operador de datos, la 1581 apropia las definiciones de responsable y encargado del tratamiento a saber:

"d) Encargado del tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento;

e) Responsable del tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos;" (Ley 1581, 2011)

Así, en materia de requisitos para el tratamiento de datos, la Ley 1581 exige el consentimiento previo, expreso e informado del titular de la información, aunque las medidas de seguridad exigidas no varían mucho entre fuentes y operadores de información. De forma principal, el ámbito de aplicación de esta ley estatutaria rige a todo "… *conjunto organizado de información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables que sea objeto* de c*ualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión"* (Ley 1581, 2011) Como es posible observar, la definición del artículo 3º se encuentra compuesta por dos conceptos más, los cuales resulta pertinente abordar para darle un mayor marco de compresión y alcance a la norma.

Así pues, el primero hace referencia a la noción de dato personal, el cual se encuentra imbuido en la misma ley y que se entiende como: "*Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables*"; mientras que el segundo se remite a la noción de tratamiento, el cual es descrito igualmente por la misma norma, como: "*Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión*". Adicionalmente, el ámbito de aplicación descrito en el artículo 2º hace múltiples referencias a la noción de bases de datos, describiendo cuáles están exentas de la aplicación de esta norma, lo que

necesariamente implicó para el legislador la necesidad de incorporar y adecuar una definición tecnológica, más que jurídica, la noción de bases de datos definida como: "*Conjunto organizado de datos personales que sea objeto de tratamiento*".

Esta definición incluida en la Ley 1581 es una restricción de lo que los operadores y fuentes manejan en el día a día como bases de datos, que tiene su origen en la informática donde se categoriza como base de datos: "*todo conjunto de información, agrupada o estructurada, en términos simples y sencillos"* (Historia de la base de datos: evolución, gestores y mas, s.f.)

A partir de esta definición es importante aclarar que en términos informáticos dato e información se usan como sinónimos de manera indistinta. De ahí que se afirme que la definición incorporada en la Ley 1581 es una restricción de la definición técnica de base de datos, al limitarlo como un "conjunto organizado de datos personales […] es decir para los efectos de esta ley sólo calificarían como bases de datos aquellas que contienen '*información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"* (Ley 1581, 2011)

Igualmente, mientras la Ley 1266 clasifica los datos en privados, semiprivados y públicos, la 1581 adiciona la categoría de dato sensible, entendido como: aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos (Ley 1581, 2011).

Sin embargo, no incluye jerarquías dentro de las distintas enunciaciones de dato sensible. Esto implica que no hay datos más sensibles que otros, tampoco se especifica qué medidas de

seguridad deben incorporarse al hacer el tratamiento de datos sensibles, excepto en el caso de datos personales de niños, niñas y adolescente donde inicialmente se prohibía el tratamiento de esta información a menos que se estuviese bajo alguno de los cinco supuestos de hecho que describe la norma: (i) tener autorización del titular, (ii) el tratamiento es necesario para salvaguardad la vida del titular, (iii) el tratamiento es realizado por una ONG, entidad sin ánimo de lucro, política o religiosa sobre los datos de personas que regularmente se relacionan con la entidad, (iv) el tratamiento del dato es necesario para la defensa de derechos a nivel judicial o (v) para fines históricos o estadísticos.

También la Ley 1581 consagra el principio de legalidad en materia de tratamiento de datos: *El tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen*; de manera que se limita la autonomía de la voluntad bajo la cual se rigió el tratamiento de datos hasta el 2011.

Conviene destacar que las leyes estatutarias 1266 y 1581 no sólo detallan todas las prerrogativas en cabeza del titular de la información, las cuales ya habían sido enunciadas en el artículo 15 de la Constitución Política, estas normas desarrollan las obligaciones que recaen en los sujetos que hacen tratamiento de datos ya previamente descritas en la jurisprudencia constitucional. La Ley 1266 prevé la posibilidad de recibir información de titulares colombianos proveniente de otros países, pero no regula la transferencia de datos personales de las personas en Colombia hacia otros países. Para este segundo caso la Ley 1581 importa al ordenamiento jurídico un concepto originado en la regulación de la Unión Europea, la noción del "*país que ofrece un nivel adecuado de protección de datos*" mediante lo dispuesto en el artículo 26 a saber:

> "*ARTÍCULO 26. PROHIBICIÓN. Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la*

materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios.[9]

Esta prohibición no regirá cuando se trate de:

a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;
b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;
c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;
d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;
e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular;
f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

PARÁGRAFO 1o. En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

PARÁGRAFO 2o. Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008."

En los primeros ocho años de vigencia de esta prerrogativa la Superintendencia de Industria y Comercio, a través de su Delegatura de Protección de Datos Personales, ha declarado como estados con nivel adecuado de protección de datos a 38 países entre los que se encuentran: "*Alemania; Australia, Austria; Bélgica; Bulgaria; Chipre; Costa Rica; Croacia; Dinamarca; Eslovaquia; Eslovenia; Estonia; España; Estados Unidos de América; Finlandia; Francia; Grecia; Hungría; Irlanda; Islandia; Italia; Japón; Letonia; Lituania; Luxemburgo; Malta; México; Noruega; Países Bajos; Perú; Polonia; Portugal; Reino Unido; República Checa; República de Corea; Rumania; Serbia; Suecia; y los países que han sido declarados con el*

[9] Subraya fuera de texto

nivel adecuado de protección por la Comisión Europea.” (Superintendencia de Industria y Comercio, 2020, pág. 20)

Este listado legitima el análisis sobre los regímenes de protección de datos que tienen otras latitudes, las cuales serán abordadas en el siguiente capítulo.

Finalmente, la Ley 1581 ordena la creación del Registro Nacional de Bases de Datos (RNBD), registro que impuso la obligación de registrar todos los mecanismos de recolección, tratamiento y eliminación de datos como mecanismo para consolidar un *directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual es administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos* (Superintendencia de Industria y Comercio, s.f.), el cual fue especificado mediante el Decreto 886 de 2014, que será abordado más adelante.

2.3.3 Ley de Acceso a la Información Pública: Ley 1712 de 2014

Como se señaló al analizar el principio de circulación restringida del dato, fue a través de la Ley 1712 de 2014 que se hizo precisa la afirmación de que un dato sea tratado o administrado por una entidad pública no implica que el dato sea de acceso público. Así las cosas, el artículo 6º de dicha norma incluye dos tipologías a la noción de dato público, a saber:

> *“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;*

e) *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;"* (Ley 1712, 2014)

Incluye, adicionalmente, un concepto que será la base del documento CONPES 3920 del 17 de abril del 2018, la política nacional de explotación de datos (Big Data) con la siguiente definición:

> "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*" (Ley 1712, 2014)

Estas clasificaciones sustentan las excepciones al derecho de acceso a la información pública, legitimando a las entidades a negarse a otorgar información a terceros si esta divulgación puede afectar derechos individuales o el interés público.

2.4 Desarrollo reglamentario

Las disposiciones anteriormente descritas deben ser reglamentadas en ejercicio de lo dispuesto en el numeral 11 del artículo 189 de la Constitución Política[10]. Así las cosas, una vez expedida la Ley 1266 del 2008, fue expedido el Decreto 1727 el 15 de mayo de 2009, el cual reglamenta la información que deben reportar las entidades a los encargados de tratamiento de los datos, como las centrales de riesgo, para que la información pueda ser considerada completa, actualizada y presentada en debida forma.

[10] *ARTICULO 189. Corresponde al Presidente de la República como Jefe de Estado, Jefe del Gobierno y Suprema Autoridad Administrativa: […] 11. Ejercer la potestad reglamentaria, mediante la expedición de los decretos, resoluciones y órdenes necesarios para la cumplida ejecución de las leyes*. (Constitución Politica, 1991)

Un año después, el Decreto 2952 del 2010 reglamentó un escenario que no fue previsto inicialmente en la legislación, el cual hace referencia a cómo debe reportarse el incumplimiento de una obligación, cuando éste ha sido causado por circunstancias de fuerza mayor, tales como el secuestro, la desaparición o el desplazamiento forzado del deudor. Posteriormente, el Régimen General de Protección de Datos Personales, la Ley 1581 de 2012, fue reglamentada parcialmente mediante Decreto 1377 del 27 de junio de 2013. En él se establece: i) el régimen de transición aplicable a las entidades que tratan datos con anterioridad a la expedición de la Ley 1581; ii) requisitos para el tratamiento de niños, niñas y adolescentes; iii) se desarrolla el deber de los responsables de datos de tener políticas de tratamiento de datos personales; iv) e incorpora en el ordenamiento jurídico colombiano un nuevo esquema de responsabilidad: el principio de responsabilidad demostrada. Posteriormente, fue expedido el Decreto 886 del 13 de mayo de 2014, que reglamenta el RNBD.

Como resultado de lo anterior se centrará la explicación en los dos principales aportes del régimen reglamentario: el principio de responsabilidad demostrada y el Registro Nacional del Bases de Datos, que se abordarán a continuación:

2.4.1 Principio de responsabilidad demostrada

Este principio ha tenido un importante desarrollo en la Organización para la Cooperación y el Desarrollo Económicos (OCDE), desde la emisión en 1980 de Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, la cual fue actualizada en 2013. En dicho documento, la OCDE describe el rol de controlador de datos como:

> *Una parte que de acuerdo con la ley doméstica es competente para decidir acerca del contenido y uso de datos personales sin importar si dicha información es recolectada, guardada, tratada o divulgada por esta parte o por un agente bajo su cargo.*[11]

Posteriormente establece:

> *El controlador de datos debe ser responsable del cumplimiento con las medidas que hagan efectivos los principios anteriormente establecidos*.[12]

En ese sentido, el rol del controlador de datos puede considerarse sinónimo del "responsable" de acuerdo con la definición establecida en la Ley 1581, este sujeto es destinatario de esta disposición que el Decreto 1377 de 2013 establece:

> "***Artículo 26.*** *Demostración. Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este Decreto, en una manera que sea proporcional a lo siguiente:*
>
> 1. *La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.*
> 2. *La naturaleza de los datos personales objeto del tratamiento.*
> 3. *El tipo de tratamiento.*
> 4. *Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.*

[11] "Data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf" (OCDE, 1980)

[12] "14. A data controller should be accountable for complying with measures which give effect to the principles stated above." (OCDE, 1980, pág. 16)

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los responsables deberán suministrar a ésta una descripción de los procedimientos usados para la recolección de los datos personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas." (Decreto 1377, 2013)

Así pues, esta responsabilidad mantiene la carga definida inicialmente por la Corte Constitucional en relación con el principio de seguridad, mientras ratifica el compromiso del Estado colombiano de neutralidad informática. Esto implica que no se impone una medida informática específica, como un software, hardware, servicio, etc. Sin embargo, para considerar que un responsable está garantizando el tratamiento de datos de acuerdo con los parámetros fijados en el ordenamiento jurídico, en el siguiente artículo se describe lo que puede entenderse por *medidas de seguridad apropiadas*, así:

"***Artículo 27***. *[…] Dichas políticas deberán garantizar:*

1. *La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este Decreto.*
2. *La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.*
3. *La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto a cualquier aspecto del tratamiento.* " (Decreto 1377, 2013)

Aunado a esto, en 2015 la Superintendencia de Industria y Comercio (SIC) emitió la *Guía para la Implementación del Principio de Responsabilidad Demostrada* (accountability) y en 2019 la SIC expidió la *Guía para la Implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales*.

Estos documentos contienen recomendaciones de la autoridad de protección de datos personales para las entidades vigiladas, que permiten tener indicaciones prácticas de las formas en las que pueden dar cuenta del cumplimiento de sus deberes como obligados en el marco del principio de la responsabilidad demostrada. Al ser recomendaciones no tienen una consecuencia jurídica explícita por su incumplimiento, pero la entidad vigilada tendría que justificar muy bien como cumple sus obligaciones a pesar de dicho incumplimiento.

En aplicación de este ordenamiento jurídico, durante 2019 la delegatura de protección de datos personales de la Superintendencia de Industria y Comercio recibió 12.741 quejas de ciudadanos que denunciaron el tratamiento de información por parte de terceros de formar indebida. Cifra que muestra un crecimiento de 36,01% frente a las recibidas en 2018. (Superintendencia de Industria y Comercio, 2020) Con el paso de los años el volumen de las quejas se ha multiplicado, al punto que en 2021 esta entidad de inspección, vigilancia y control recibió 28.610 quejas que, a su vez, representó un aumento 74.49% respecto de las radicadas en 2020. La mayoría de estas quejas se centran en el tratamiento de datos financieros. (Superintendencia de Industria y Comercio, 2022)

En este orden de ideas, la SIC en los últimos años ha acumulado una valiosa experiencia, que le ha servido para priorizar las entidades con mayores riesgos de incumplimientos de las cargas establecidas en el régimen de protección de datos personales para Colombia. En ese sentido, para que se considere que una entidad ha adoptado un Plan Integral de Gestión de Datos

Personales, es necesario que se describan procedimientos que van en concordancia con lo solicitado en el RNBD, tales como la creación de una estructura administrativa con recursos para llevar a cabo este plan integral de gestión de datos, el cual inicia con la formulación de una política de tratamiento de datos, pero se extiende a la definición de sujetos y cargos responsables de implementar los debidos procedimientos, así como también inventariar cada espacio de tratamiento de datos, realizar informes, hallazgos y educar a personal de toda la organización, para la real efectividad de todo el diseño desde la arquitectura institucional que requiere el plan integral de gestión de datos.

2.4.2 Registro Nacional de Bases de Datos

Este registro fue creado en el artículo 25 de la Ley 1581, como el directorio público de las bases de datos sujetas a tratamiento que operan en Colombia, el cual es de libre consulta para los ciudadanos. El mismo artículo señala: "*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.*" (Ley 1581, 2011)

En concordancia, la Corte Constitucional en la Sentencia C-748 de 2011 aclara que este registro "*debe permitir a cualquier persona determinar quién está haciendo tratamiento de sus datos personales para de esa forma garantizar que la persona pueda tener un control efectivo sobre sus datos personales al poder conocer clara y certeramente en qué bases se manejan sus datos personales*".

Para dar cumplimiento a esta obligación el Gobierno colombiano profirió el Decreto 886 de 2014, dentro del cual se señala que el registro debe hacerse por cada una de las bases de datos sobre las que se está haciendo tratamiento señalando en cada caso:

1. "*Datos de identificación, ubicación y contacto del responsable del tratamiento de la base de datos;*
2. *Datos de identificación, ubicación y contacto del o de los Encargados del Tratamiento de la base de datos;*
3. *Canales para que los titulares ejerzan sus derechos;*
4. *Nombre y finalidad de la base de datos;*
5. *Forma de Tratamiento de la base de datos (manual y/o automatizada), y*
6. *Política de Tratamiento de la información*." (Decreto 886, 2014)

Puede entonces observarse la concordancia entre la información que debe ser reportada a la autoridad encargada por velar y administrar este registro público, que es la misma entidad que puede hacer requerimientos, recomendaciones o imponer sanciones en caso de disconformidad con el principio de responsabilidad demostrada. Con ello, el cumplimiento de esta responsabilidad se demuestra, inicialmente, al cumplir efectivamente la carga del Registro Nacional de Bases de Datos.

Pero esta actividad no es la única para cumplir con el principio. De ahí que la entidad de vigilancia y control tuviese que expedir guías para la implementación del principio de responsabilidad demostrada.

Así pues, en el ordenamiento jurídico existe un marco constitucional y legal que busca garantizar la protección de datos de las personas inspirado inicialmente de reglas extraídas de casos concretos hasta la emisión de las leyes estatutarias previamente analizadas y su subsecuente reglamentación. No obstante, es importante traer a colación el diagnóstico que

refleja el documento CONPES 3920 del 17 de abril del 2018, que establece la política nacional de explotación de datos (Big Data) donde se identifican los siguientes retos en materia de legislación:

- "*Protección del titular: la Ley 1581 de 2012 impone la carga de protección al titular del dato, quien debe consentir el uso del mismo. En el contexto de masificación de bienes y servicios que recolectan datos personales en todos los ámbitos de desenvolvimiento de una persona, la manifestación de este consentimiento se ha reducido a marcar una casilla manifestando haber leído y entendido los extensos términos y condiciones so pena de desistir del bien o servicio que solicita la autorización para su acceso y uso.*
- *Individualización a partir de datos impersonales: las normas fueron proferidas en un contexto donde no era técnicamente posible la individualización a partir de ciertos datos impersonales. Por tanto, no prevén claramente el tratamiento que debe darse a los datos anonimizados, los cuales, unidos con otros de naturaleza pública, pueden brindar información de una persona determinada o determinable. Tampoco se ha previsto el procedimiento que debe seguirse respecto a los datos impersonales, los cuales, luego de haber sido analizados de manera legal, se convierten en personales*" (CONPES, Consejo Nacional de Política Economica y Social, 2018, págs. 60-61)

Estos retos serán relevantes al contrastar la perspectiva regulatoria con el tráfico jurídico y mercantil de los datos en el sector privado y público, a través de la utilidad que generan los procesos analíticos sobre la información de las personas en la era del Big Data.

3. Capítulo II - Protección de datos personales a escala internacional

3.1 Introducción

Para Castells, el impacto social de la tecnología está potencializada por factores adicionales al bien o servicio tecnológico. Ejemplo de ello es: "*aunque la imprenta afectó de forma considerable a las sociedades europeas en la Edad Moderna, al igual que a la China medieval en menor medida, sus efectos quedaron hasta cierto punto limitados por el analfabetismo extendido de la población y por la baja intensidad que tenía la información en la estructura productiva. La sociedad industrial, al educar a los ciudadanos y organizar gradualmente la economía en torno al conocimiento y a la información, preparó el terreno para que la mente humana contara con las facultades necesarias cuando se dispuso de las nuevas tecnologías de la información"*. (Castells, 2006, pág. 57)

Así pues, mientras en 1993 sólo el 0.251% de la población mundial usaba internet, para 2018 el porcentaje ascendía al 49.72%, y en Colombia dicha proporción llegaba al 64% (Unión Internacional de Telecomunicaciones, s.f.). Este indicador es usado por entidades como la OCDE y el Banco Mundial, como indicio de desarrollo en los países, pero también representa la cantidad de población que potencialmente podrían ser impactadas en caso de proteger o exponer los datos personales que circulan en esta red (Amer & Noujaim, 2019)

3.2 Protección de datos en el mundo

La protección de datos es abordada por la doctrina y los distintos países como un derecho humano, derecho fundamental, que históricamente se deriva del derecho de propiedad ya conocido y regulado por los romanos, derecho del cual, se ha consagrado también el derecho a la intimidad o privacidad, este último entendido en algunos ordenamientos, como el estadounidense, como sinónimo de protección de datos o *privacy.*

Desde el ámbito internacional la primera norma que establece una regulación sobre el tratamiento de datos personales es la Declaración Universal de Derechos Humanos, adoptada y proclamada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948, cuyo artículo 12 dispone:

> *Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*.

Posteriormente, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado también por la Asamblea General de las Naciones Unidas, el 16 de diciembre de 1966[13,] y la Resolución 2450 del 19 de diciembre de 1968 de la Asamblea General de Naciones Unidas, sobre Derechos Humanos y Progresos Científicos y Tecnológicos, expresan preocupación en relación con "*el respeto a la vida privada de los individuos y a la integridad y la soberanía de las naciones ante los progresos de las técnicas de registro y de otra índole*; (Asamblea General de las Naciones Unidas, 1968)".

Consecutivamente, la Organización para la Cooperación y el Desarrollo Económicos – OCDE- desde 1980, con el fin de apoyar los tres principios que caracterizan a sus Estados miembros (democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas) ha emitido una serie de directrices en materia de Protección de Datos que se concentran principalmente en tres instrumentos:

1) Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales (1980): Efectivas desde el 23 de septiembre de 1980, parten de la necesidad de la unanimidad internacional para regular la recogida y gestión de información

[13] 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

personal. Pretenden abarcan todos los medios desde computadoras locales a redes con complejas ramificaciones nacionales e internacionales, todos los tipos de procesamiento de datos personales y todas las categorías de datos (desde el más trivial al más delicado). Los principios se pueden aplicar en los ámbitos nacional e internacional. A lo largo de los años se han utilizado en gran número de instrumentos de regulación nacional o de autorregulación, como por ejemplo la Ley 1266 de 2008 en Colombia.

2) Declaración sobre flujos de datos transfronterizos (1985), adoptada el 11 de abril de 1985. Este documento aborda las cuestiones políticas que surgen del flujo de datos personales más allá de las fronteras nacionales. Al adoptar esta declaración, los gobiernos de la OCDE reafirmaron su compromiso por desarrollar enfoques comunes ante las cuestiones de flujos de datos transfronterizos y, si se presenta la ocasión, desarrollar soluciones armonizadas.
3) Declaración ministerial sobre la protección de la privacidad de las redes globales (1998). Posteriormente, en la conferencia ministerial de la OCDE "Un mundo sin fronteras: determinación del potencial del comercio electrónico", celebrada en 1998 en Ottawa, los ministros reafirmaron "*su compromiso sobre la protección de la privacidad de las redes globales para garantizar el respeto de importantes derechos, generar confianza en las redes globales y evitar restricciones innecesarias en los flujos transfronterizos de datos personales*." Declararon concretamente que "*trabajarían para vincular los diferentes enfoques adoptados por los países miembros con vistas a asegurar la protección de la privacidad en las redes globales basándose en las directrices de privacidad de la OCDE*." (OCDE, 1980)

Con el fin de ser lo más adaptables posibles a la legislación de cada estado, la OCDE (1980) presenta sus directrices a través de los siguientes principios:

3.2.1. **Limitación de la recogida:** se centra en la forma como se obtiene el dato personal limitándola a medios que califica como “legales y justos” y siempre que se pueda con autorización del titular de los mismos.

3.2.2. Calidad de los datos: se relaciona con los principios de finalidad y veracidad del régimen jurídico colombiano. En ese sentido, se ratifica que la recopilación de la información debe ser relevante para un propósito específico y siempre exacta, completa y actual.

3.2.3. Especificación del propósito: describe el momento en debe informarse al titular de los datos el objetivo o uso que rige la obtención de estos, también delimita el alcance del tratamiento de datos al uso u objetivo que fue informado al titular.

3.2.4. Limitación de uso: puede ser identificado con el principio de circulación restringida del dato y el principio de libertad del régimen colombiano pues prohíbe expresamente el uso o divulgación de los datos personales para uso no autorizados salvo autorización del titular u orden de autoridad competente.

3.2.5. Salvaguardas de seguridad: es equiparable a los principios de seguridad y responsabilidad demostrada, donde se impone la carga de implementar medidas razonables que impidan violaciones al régimen de tratamiento de datos.

3.2.6. Transparencia: impone la obligación de que en el régimen colombiano se cumpla con la formulación de políticas de tratamientos de datos, adicionalmente, los responsables del tratamiento deben tener una manera ágil se identificar quien controla datos y dónde está ubicado.

3.2.7. Participación individual: En este principio se consagran los derechos de los titulares de la información a conocer y solicitar la rectificación de su información, así como la forma de ejercer este derecho.

3.2.8. Responsabilidad: Consagra sobre el controlador el deber de dar cumplimiento a las medidas que imponen estos principios.

Inspirados por estas directrices, que no tienen fuerza vinculante directa, en 1989 se creó un foro multilateral de negociación en temas relativos al intercambio comercial, coordinación y cooperación entre las economías, el cual incluye países como Australia, Canadá, Chile, Corea, Estados Unidos de América, Filipinas, Indonesia, Japón, México, Nueva Zelanda, Perú, Rusia y Vietnam llamado APEC (Asia Pacific Economic Cooperation). Esta entidad emitió en noviembre de 2004 su propio marco de privacidad para facilitar la trasferencia de datos con fines comerciales entre los Estados del APEC, por lo cual este marco regulatorio es más flexible que el establecido por la Unión Europea.

Se observa también que en el seno de la Organización de Estados Americanos (OEA) se expidieron el 31 de diciembre del 2021 los principios actualizados sobre la Privacidad y la Protección de Datos Personales, aprobados por resolución AG/RES. 2974 (LI-O/21) de fecha 11 de noviembre de 2021. Estos buscan ser un marco general para los ordenamientos que cada estado miembro emita en este asunto, eso sí, bajo la premisa de que no son directamente obligatorios si no que este es un instrumento de *Soft Law*. (Secretaría de Asuntos Jurídicos, 2022)

La mayoría de los principios que se consagran en este documento ya hacen parte del ordenamiento jurídico colombiano: finalidad, libertad, transparencia, confidencialidad, seguridad, calidad, etc. No obstante, llama la atención que en esta resolución se trate a los principios sobre Privacidad y la Protección de Datos personales como un asunto propio del derecho internacional privado, sin darse mayor contexto de las razones de esta categorización.

Finalmente, en el marco del Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado del 1 al 6 de junio de 2003, con la asistencia de los representantes de 14 países

iberoamericanos se fundó la Red Iberoamericana de Protección de Datos (RIPD) con el objetivo de ser un "*foro integrador de los diversos actores, tanto del sector público como privado, que desarrollen iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica, con la finalidad de fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos, así como promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho*." (Red Iberoamericana de Protección de Datos, s.f.)

En cumplimiento de este objetivo, la Red Iberoamericana de Protección de Datos personales ha impulsado la promulgación de las leyes de protección de datos personales en más de 8 países en Suramérica, entre ellos las leyes estatutarias 1266 y 1581 para el caso de Colombia, así como proyectos legislativos en otros cuatro países. Es importante señalar que en esta instancia no solo participan las entidades de encargadas de la inspección, vigilancia y control de las normas de protección de datos personales de cada Estado miembro, sino que además participan en calidad de observadores la Organización de Estados Americanos (OEA), el Supervisor Europeo de Protección de Datos y el Comité Consultorio del Convenio 108 del Consejo de Europa, de forma que puede advertirse una simetría entre los *Estándares de Protección de Datos Personales para los Estados Iberoamericanos* (2017) y la norma comunitaria Europea. (Red Iberoamericana de Protección de Datos (RIPD), s.f.).

Teniendo en cuenta esta simetría impulsada por la Red Iberoamericana de Protección de Datos y la importancia de los estándares de protección de datos personales de la Unión europea, a continuación, será analizado el respectivo régimen y su relación con la legislación colombiana.

3.3 Protección de datos en la Unión Europea

De conformidad con la Sentencia C-748 de 2011 de la Corte Constitucional colombiana, fue en el sistema europeo donde se empezó a plantear el habeas data como un derecho fundamental autónomo, en primer lugar, a través del artículo 8º del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, en 1950. En segundo lugar, en 1967, cuando el Consejo de Europa convocó una comisión consultiva para estudiar los riesgos que las tecnologías de la información generan sobre los derechos de las personas. En virtud de ello se expidió, en 1968, la Resolución 509 sobre los derechos humanos y los nuevos logros científicos y técnicos, en la que se hizo un llamado a la protección de la privacidad frente a las nuevas tecnologías. (Sentencia C-748, 2011)

Todos estos cuerpos normativos no tienen una fuerza vinculante expresa para los Estados, motivo por el cual se hace necesario un análisis de las normas que sí tienen una fuerza vinculante expresa. A la fecha, la más importante de todas y referente internacional es la Directiva Europea (Agencia de los Derechos Fundamentales de la Unión Europea, 2014) aunque esta directiva fue revisada en 2016, particularmente con ocasión a una sentencia de 2015 de la Corte Europea de Derechos Humanos.

Sus antecedentes se remontan al 28 de enero 1981, cuando el Consejo de Europa adoptó la “Convención para la Protección de los Individuos en Relación con el Procesamiento Automático de Datos Personales” también conocido como el "Convenio de Estrasburgo" o "Convenio 108". Es por la fecha de celebración de este convenio que la Unión Europea celebra el 28 de enero como “El día mundial de la Protección de Datos”, como parte de un programa para concientizar a los ciudadanos europeos sobre la información que divulgan en medios como internet.

En desarrollo de esta convención se expidió la Directiva N° 95/46/CE del Parlamento Europeo y del Consejo del 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, estableciendo un régimen normativo exhaustivo en la materia tanto para casos de tratamiento realizado manualmente como de forma automatizada, aplicable tanto en el sector público como en el privado, obligatoria en todos los estados miembros de la Unión Europea. Esta directiva en particular influyó directamente a nivel mundial en materia de producción legislativa, como fue el caso de Colombia, particularmente por el artículo 25, apartado 1, de la Directiva 95 N° 95/46/CE, el cual establece:

"la libre circulación de datos a terceros países con un nivel ***adecuado*** *de protección de datos. El requisito de nivel adecuado en lugar del de equivalencia posibilita que se distingan diferentes formas de aplicar la protección de datos. Según el artículo 25, apartado 6, de la Directiva, la Comisión Europea es competente para valorar el nivel de protección de datos en los países extranjeros mediante decisiones sobre el carácter adecuado de la protección y realizar consultas sobre la evaluación al Grupo del artículo 29, quien ha contribuido sustancialmente a la interpretación de los artículos 25 y 26.*

Una conclusión de que existe un carácter adecuado por parte de la Comisión tiene efectos vinculantes. Si la Comisión Europea publica en el Diario Oficial de la Unión Europea una decisión sobre el carácter adecuado de la protección para un determinado país, todos los países miembros del y sus órganos estarán obligados a seguir la decisión, lo cual significa que los datos pueden circular a dicho país, sin seguir un procedimiento de comprobación o de autorización ante las autoridades nacionales (Agencia de los Derechos Fundamentales de la Unión Europea, 2014)

En materia de tratamiento de datos, como se señaló en el capítulo anterior, la Ley 1581 de Colombia apropia la categoría de "nivel adecuado de protección de datos" implementado por la Directiva 95/46/CE que a través de la Circular Externa 005 de 2017 establece los requisitos para que un Estado sea incluido dentro del grupo de países que son considerados con un nivel adecuado de protección de datos, estos son:

a) Tener normas aplicables al tratamiento de datos personales.
b) Consagración normativa de principios aplicables al tratamiento de Datos, entre otros: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
c) Consagración normativa de los derechos de los titulares.
d) Consagración normativa de deberes de los responsables y encargados
e) Existencia de medios y vías judiciales y administrativas para garantizar la tutela efectiva de los derechos de los titulares y exigir el cumplimiento de la ley
f) Existencia de autoridades encargadas de la supervisión del tema.

No obstante, a la luz del reglamento de la Unión Europea será necesario hacer una revisión de la legislación interna, pues Colombia aún no está calificado de forma recíproca como un Estado con nivel adecuado de protección de datos.

Es importante señalar que con el Tratado de Lisboa en diciembre de 2009, la Carta de Derechos Fundamentales de la Unión Europea pasó a ser jurídicamente vinculante y, con ello, se consolidó el derecho a la protección de los datos personales a la categoría de derecho fundamental independiente. Esto, unido a la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos (Agencia de los Derechos Fundamentales de la Unión Europea, 2014) sirvieron como incentivos para la revisión de la directiva 95 N° 95/46/CE, logrando como consecuencia la expedición del Reglamento (UE)

2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a su libre circulación y que deroga la Directiva 95/46/CE, este reglamento entró en vigor en mayo del 2018.

Esta directiva incluyó importantes novedades exigibles a todos los operadores de información dentro de la unión europea y para aquellos terceros países que voluntariamente acepten esta regulación. Algunas novedades establecidas en la Directiva se tratarán a continuación:

3.3.1 Regulación de las decisiones automatizadas

Esta directiva impone la obligación a los responsables de informar a los titulares cuando y como una decisión será tomada de forma automatizada o producto de la elaboración de perfiles, dando la potestad al titular de solicitar que una persona revise dicha decisión.

3.3.2 Derecho al olvido

Entendido como la prerrogativa del titular de la información de solicitar la eliminación de la información que un responsable tenga, cabe señalar que esta potestad está limitada cuando el tratamiento se hace en cumplimiento de un deber legal, o con fines científicos y estadístico, en los casos en que deba protegerse la libertad de expresión y de información, o cuando exista un reclamo en torno a dichos datos.

3.3.3 Derecho a portabilidad

Entendido como la posibilidad de que el titular solicite a un responsable la información que tenga del titular mismo para entregarla a otro responsable, o que la información sea entregada directamente entre un responsable a otro, bajo el supuesto de que el tratamiento está sustentado en el consentimiento del titular, el tratamiento susceptible de portabilidad debe hacerse en

medios automatizados y la portabilidad de los datos personales no puede autorizarse si con ellos se vulnera el interés público.

3.3.4 Modificación de las condiciones de acceso a la información personal

Se impone la obligación a los responsables de diseñar mecanismos expeditos de entrega, rectificación y supresión de la información, este último bajo las condiciones del derecho al olvido.

3.3.5 Imposición de acreditar consentimiento inequívoco

Además de tener soporte del otorgamiento de la autorización, se impone a los responsables que el consentimiento para el tratamiento de datos personales sea diferenciable de la aceptación de otros términos, clausulas y condiciones en un lenguaje claro y sencillo.

3.3.6 Mayor rigurosidad en materia de seguridad

Teniendo en cuenta el contexto en el que se hace el tratamiento se impone a los responsables la obligación de seudonimizar[14] y cifrar la información personal de forma que fortalezca la circulación restringida de la información, también se regula como notificar a los titulares en caso de la materialización de una violación a los protocolos de seguridad.

3.3.7 Alternativas para transferencia internacional de datos

Si bien se mantiene la exigencia de que un país tenga un adecuado nivel de protección de datos para autorizar el tratamiento de datos de ciudadanos de la Unión Europea, este reglamento da la posibilidad de que la entidad de control autorice transferencias de datos a Estados que aún no tienen esta clasificación. Si el Estado o los interesados ofrecen garantía adecuadas, en este último caso dando fuerza vinculante a los reglamentos corporativos y de autorregulación que

[14] Definida en el Reglamento General de Datos Personales como una separación de la información que impida que los individuos sean identificados o identificables salvo que se cuente con información adicional.

puede tener un sujeto de derecho privado como Meta[15], pero que lo hace en el marco de su autonomía pues la ley nacional que le rige no le exige estas garantías.

En concordancia, desde el ámbito territorial de validez, éste reglamento es exigible no sólo a los Estados de la Unión Europea y a sus instituciones, sino también a los responsables y encargados del tratamiento de datos que sean de la Unión Europea, aun cuando el tratamiento no se ejecute en la unión. Por otro lado, aunque en este reglamento no se habla de titular del dato si no del interesado, se extiende la aplicación del reglamento, si el tratamiento de datos versa sobre interesados residentes en la Unión Europea, si y sólo si es sobre bienes y servicios ofrecidos en la unión o si se tiene control del comportamiento del responsable en la medida en que esté en la unión.

Con este contexto normativo, es preciso señalar que dentro de la explotación masiva de datos, Big Data, son requeridas amplias capacidades de almacenamiento y procesamiento de la información, lo cual es costoso lograr con servidores físicos pues requieren de una inversión sustancial para garantizar que cuenten con el personal y las condiciones técnicas, de conservación, mantenimiento y seguridad idóneas para su funcionamiento, aunado a la inversión adicional que demandarían cada vez que se deba ampliar la capacidad de almacenamiento y/o procesamiento. (Arcitura™ Education Inc., s.f.)

Dichos inconvenientes sirvieron de nicho para la oferta de servicios de almacenamiento en la nube, a los cuales se accede a través de internet conectándose con proveedores dedicados exclusivamente a cobrar por el almacenamiento y el procesamiento que sea efectivamente utilizado por cada cliente mientras estos asumen la responsabilidad sobre la custodia, mejora y conservación de grandes servidores en espacios que denominan Data Centers, esta alternativa permitió la oferta de una nueva medida de seguridad de la información: la posibilidad de

[15] Antes Facebook

guardar un soporte o respaldo de la información, la cual es más de un data center. Con esto la información se protege de riesgos como la guerra o problemas de orden público que puedan destruir una de las instalaciones del proveedor.

Conforme lo refleja el mapa mundial de Data Centers (Cloud Servers, s.f.), en Colombia solo hay cinco compañías que ofertan este servicio, mientras que la mayoría de los proveedores han ubicado sus Data Centers entre Estados Unidos y Europa, entre ellos, los oferentes más relevantes de este mercado: Google, Amazon y Microsoft. Esto implica que es más probable que cuando una persona contrata los servicios de almacenamiento y procesamiento de su información en nube este cargándolos en un data center que no está regido directamente por la normatividad colombiana, incurriendo en una transferencia internacional de datos. Ante esta realidad, países como Japón y Alemania han optado por tener Data Centers exclusivos para el tratamiento de datos de sus nacionales, mientras que en el caso colombiano esta alternativa no se ha previsto.

Esta transferencia internacional de datos hace pertinente contrastar las disposiciones internacionales y la normatividad de los entornos donde se concentran la mayor parte de los Data Centers en el mundo, y que influencian la forma en que se deben tratar datos personales, esto es, la Unión Europea y también Estados Unidos, toda vez que son en estos espacios donde se ubican la mayoría de los data center del mundo (Cloud Servers, s.f.).

3.4 Protección de datos: Estados Unidos

En primer lugar, debe tenerse en cuenta que la protección de datos personales en este Estado federal se conoce como *Privacy* y es tratado como un derecho del consumidor, a diferencia del régimen europeo y colombiano que lo consideran derecho humano fundamental u autónomo. Actualmente, Estados Unidos no tiene una norma especial que regule a nivel federal el uso y

transferencia de los datos personales; no obstante, sí tiene una considerable cantidad de normas que regulan el tema a nivel sectorial.

En segundo lugar, no existe una entidad que a nivel nacional vigile el cumplimiento de estas normas, por lo que la Federal Trade Commission -FTC- se ha abrogado esta función con ocasión a sus funciones de vigilancia sobre la mayor parte de los mercados, pero siempre bajo la guía y autorización de las normas sectoriales previamente mencionadas, en particular en materia de prácticas restrictivas del mercado y competencia desleal.

Dado el modelo de Estado federado a nivel interno también existe una sobreproducción normativa que incide en temas tan cruciales como la existencia de varias definiciones de dato personal. La FTC define el dato como la información que puede ser usada razonablemente para contactar o identificar a una persona, incluyendo dirección IP o códigos IMEI de un dispositivo electrónico, mientras que para algunos de los estados federados esta definición incluye información que en sí misma no identifica al titular.

Tampoco existe una delimitación general de lo que se entiende como información sensible (información que debe tener medidas especiales de protección y de tratamiento) y en materia de transferencia de datos existe el requisito unificado de tener la autorización del titular. Por ello, el receptor de los datos deberá asumir las mismas obligaciones a las que esté sujeto el transferente en materia de tratamiento de datos. (Berman D. , 2017). Sin embargo, un gran avance se dio en abril del 2018, año en el que 48 de los 50 Estados profirieron leyes que exigen la notificación de fallas de seguridad que involucren información personal, exceptuándose solamente los estados de Alabama y Dakota del Sur. (Leuan Jolly, 2017).

En consecuencia, bajo este marco legal, Estados Unidos no cumple con los parámetros para ser catalogado como Estado con un nivel adecuado de protección. No obstante, dado su protagonismo en la industria de explotación masiva de datos y de los efectos comerciales,

económicos y sociales que se darían con ocasión a una aplicación restrictiva del artículo 25 de la Directiva 95 N° 95/46/CE, la Comisión Europea y Estados Unidos acordaron la aplicación de una legislación llamada Safe Harbor en 1998, la cual consiste en un marco de "puerto seguro" que permitía a las empresas firmantes de Estados Unidos la transferencia de datos a través del Atlántico, siempre y cuando se cumplan una serie de principios de privacidad. Ello no impedía que cada uno de los Estados pertenecientes a la Unión Europea pudiese exigir mayores condiciones a las establecidas por la unión. (Martin, 2015)

A pesar de lo anterior, debe reiterarse que, con el Tratado de Lisboa en diciembre de 2009, la Carta de Derechos Fundamentales de la Unión Europea pasó a ser jurídicamente vinculante y, con ello, se consolidó el derecho a la protección de los datos personales a la categoría de derecho fundamental. Esto permitió que la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos (Agencia de los Derechos Fundamentales de la Unión Europea, 2014), en particular la Sentencia del 6 de octubre de 2015 declarara la nulidad de la llamada "Safe Harbor". En ese sentido, Estados Unidos no se encuentra en el listado de países con un nivel adecuado de protección de datos.

Pero, como se describió previamente, la ausencia de esta clasificación no necesariamente implica que las compañías estadounidenses estén impedidas para tratar datos personales de ciudadanos de la Unión Europea. En el marco de los artículos 46 y 47, este organismo dio reconocimiento y validez a las normas y políticas corporativas que estos actores de derecho privado pueden acreditar como garantías de un adecuado tratamiento de datos. Este fenómeno es un fortalecimiento de uno de los factores de la globalización y del poder que han alcanzado estas empresas, quienes de forma reglada tienen la posibilidad de tratar datos de ciudadanos europeos, a pesar de que la regulación de su país se considere insuficiente para el estar del Reglamento General Europeo.

De otro lado, también se considera pertinente incluir en el análisis el Régimen de Protección del Datos de la República Popular de China, pues este régimen prioriza los intereses del Estado sobre los intereses de responsables e individuos. Aquí es importante resaltar que, conforme fue analizado en esta sección, el régimen estadounidense privilegia a quienes hacen tratamiento de datos personales, al no dar un marco general de garantías a los derechos fundamentales individuos, mientras el régimen de la Unión Europea privilegia la aplicación de derechos fundamentales a favor de los intereses de los individuos. De esta forma, en el mundo existen tres regímenes de protección de datos que compiten dentro del mercado global, razón por la cual es necesario abordar el régimen de protección de datos en China.

3.5 Protección de datos en China

De conformidad con el mapa de data centers (s.f.), en China sólo se ubican seis datacenters, por lo que en principio su régimen de protección de datos no parecería relevante para ser analizado. A pesar de ello, de acuerdo con la información del del Banco Mundial (s.f.), este país produjo en 2019 el 16.8% del PIB Mundial, siendo la segunda economía más productiva después de Estados Unidos, y el principal exportador de bienes del mundo, con US$2.498 miles de millones, de los cuales se resalta:

a) El 9% que correspondió a *teléfonos, incluidos los teléfonos móviles (celulares) y los de otras redes inalámbricas; los demás aparatos para emisión, transmisión o recepción de voz, imagen u otros datos, incluidos los de comunicación en red con o sin cable (tales como redes locales (LAN) o extendidas (WAN)), distintos de los aparatos de transmisión o recepción de las partidas*.
b) El 5.9% en *máquinas automáticas para tratamiento o procesamiento de datos y sus unidades; lectores magnéticos u ópticos, máquinas para registro de datos sobre soporte en forma codificada y máquinas para tratamiento o procesamiento de estos datos, no expresados ni comprendidos en otra parte*.

c) El 4.1% en *circuitos electrónicos integrados.*

Para el caso de Colombia, el 20.84% de las importaciones de 2019 fueron de origen chino (Oficina de Estudios Económicos, Mincit., 2020). Además, este país se está convirtiendo de forma más seguida en un aliado de Colombia, sobre todo en proyectos de infraestructura.

Como previamente se señaló, el modelo político de este Estado privilegia el interés público sobre el particular, lo cual se evidencia en que desde junio de 2017 entró en vigor en este Estado una Ley de Ciberseguridad (Adrogue & Fernandez, 2021), instrumento que dota de legitimidad la puesta en funcionamiento de uno de los más fuertes regímenes de vigilancia sobre los ciudadanos y lo que ellos consultan en internet (Zuboff, 2019).

Una de las formas técnicas con las que se hace efectiva esta norma jurídica es conocido como el *gran firewall.* Inspirado en la Gran Muralla, esta herramienta es un escudo que impide el funcionamiento de aplicaciones como Facebook o WhatsApp en territorio chino dificultando en la medida de lo posible que actores de otros países como Estados Unidos tengan fácil acceso a hacer tratamiento de datos de ciudadanos chinos, aunque este tratamiento intente hacerse no de forma estatal si no desde el sector privado (Quinn, 2017).

Este contexto cobra relevancia teniendo en cuenta que el 21 de mayo de 2019 Estados Unidos emitió una orden ejecutiva con la prohibición a las compañías estadounidenses de tener relaciones comerciales con la compañía china Huawei y sus subsidiarias, uno de los principales fabricantes de China. Esto, a menos que se cuente con autorización del Departamento de Comercio, al considerar que esta compañía era un riesgo para la seguridad nacional pues presuntamente interceptó comunicaciones y datos a través de las antenas que fabrican para la prestación del servicio de internet y los compartió con el gobierno chino, calificando así como un riesgo para la seguridad del gobierno de Estados Unidos (Zhang, 2020).

Esta sanción puso los reflectores del mundo en la cantidad de información mundial que está a disposición del gigante asiático, pues no se restringe a la de sus aproximadamente 1.398 millones de habitantes, por lo cual también surgieron interrogantes por las aplicaciones y derechos que se pueden ejercer para proteger los datos de las personas a disposición de este Estado.

Expuesto lo anterior, preocupa que en este gigante de la economía mundial no existió durante mucho tiempo una ley general de protección de datos personales y, en consecuencia, la responsabilidad se interpretaba con fundamento en la ley civil o en la responsabilidad civil, ya sea contractual o extracontractual. (Berman D. , 2017). Por lo mismo, no existía una autoridad nacional a cargo de velar por el cumplimiento de normas de protección de datos, lo que impedía transferir o recibir datos de titulares de la unión europea, al no cumplir con las garantías mínimas que impone el régimen de protección de datos de esta organización. (Ning & Wu, 2020)

Aunada a la sanción de Huawei, la exclusión de autorización para tratar datos personales de ciudadanos europeos como consecuencia de la entrada en vigor en 2018 del actual régimen de protección de datos personales de la Unión Europea, en Estados Unidos vetaron aplicaciones de origen chino tales como Tik Tok y Wechat, por acusaciones similares a las realizadas a Huawei, las cuales parecen haber ejercido la presión internacional necesaria. Esto pareció caer en terreno fértil, pues el 21 de octubre del 2020 el Gobierno chino puso a disposición de público un borrador de régimen de protección de datos personales inspirado en el régimen de protección de datos de la Unión Europea y dentro de los que se resalta su ámbito de aplicación sobre todas las personas, ciudadanas o no que se encuentre en territorio chino. Así como de forma extraterritorial para todas las personas naturales o jurídicas que deseen hacer tratamiento de datos de personas en China para proveerles bienes o servicios, hacer análisis del

comportamiento de sujetos de datos en China o cualquier otra circunstancias prevista por las leyes y regulaciones de este país (Yin & Zhang, 2020).

Este proyecto llevó al nacimiento de la PIPL o Ley de Protección de Información Personal aprobada por la Asamblea Popular el pasado 20 de agosto de 2021 y que entró en vigor en noviembre del mismo año, como el proyecto publicado en 2020. Con esta ley, la República Popular de China muestra evidencias de su intención de tener un adecuado nivel de protección de datos personales enfocando esta norma ya no en el interés público si no en los derechos de los titulares y los deberes de los responsables.

Esta norma debe interpretarse en conjunto con la Ley de ciberseguridad y la ley de seguridad de datos, aprobada el 10 de junio del 2021, y cuya vigencia inicio en septiembre de dicha anualidad. Esta norma es la respuesta expresa a la presión que las compañías y el estado chino recibieron de forma contundente en 2019, en especial desde Estados Unidos, pues en ella se regula la transferencia internacional de datos, y se incluyen unos primeros estándares para aquellos que hacen tratamiento de datos personales. De forma especial, la ley legitima la respuesta de la República Popular de China ante actos restrictivos, discriminatorios en áreas como la inversión, tecnología, tratamiento de datos y/o comercio por parte de otros estados.

4. Conclusiones

Una vez contrastadas estas diversas formas de abordar la protección de datos personales, para finalizar este estudio se considera pertinente resaltar las siguientes conclusiones:

1. El Régimen de Protección de Datos de Colombia se inclina por seguir el Régimen de Protección de Datos de la Unión Europea, que busca ante todo la protección de los derechos fundamentales de los individuos.
2. No obstante lo anterior, el legislador colombiano está en mora de incluir en el ordenamiento jurídico interno disposiciones que impongan estándares de seguridad que aplican directamente al tratamiento de grandes volúmenes de datos, como la obligación de anonimización, ya previstos en la regulación europea.
3. A pesar de que la Unión Europea no considera a Estados Unidos como un país con un nivel adecuado de protección, éste estándar es más bajo que el utilizado para Colombia, pues Estados Unidos ya recibió este reconocimiento.
4. A pesar de que la República Popular de China tampoco ha sido reconocida con un nivel adecuado de protección, el régimen jurídico colombiano autoriza a las compañías de este país a tratar datos personales de los ciudadanos colombianos si sus normas corporativas dan evidencia del cumplimiento del régimen de protección de datos de Colombia.
5. La tardanza en la actualización de los derechos de ciudadanos en este entorno de Explotación Masiva de Datos favorece la desprotección de los ciudadanos ante perfilamientos y decisiones automatizadas pues la impugnación de estos escenarios no está previsto en el régimen actual.

5. Bibliografía

Adrogue, M., & Fernandez, D. (8 de Septiembre de 2021). *China aprueba la Ley de Seguridad de Datos*. Obtenido de Asociación Imternacional de Profesionales de Privacidad - iapp- : https://iapp.org/news/a/china-aprueba-la-ley-de-seguridad-de-datos/

Agencia de los Derechos Fundamentales de la Unión Europea. (Abril de 2014). *Manual de legislación europea en materia de la protección de datos.* Obtenido de Consejo de Europa: https://rm.coe.int/16806ae663

Alianza Caoba. (2016). *¿QUÉ SON LOS DATOS ABIERTOS?* Obtenido de http://alianzacaoba.co: http://alianzacaoba.co/inicio/mas-noticias-big-data-y-data-analytics-en-colombia-y-el-mundo/los-datos-abiertos/

Amer, K., & Noujaim, J. (Dirección). (2019). *Nada es privado* [Película].

Arcitura™ Education Inc. (s.f.). *Fundamentos de Big Data.* Obtenido de Big Data Science School sitio web: http://www.bigdatascienceschool.com/

Asamblea General de las Naciones Unidas. (19 de Diciembre de 1968). *Resolución 2450 de 1968.* Obtenido de Organización de Naciones Unidas: http://www.un.org/es/comun/docs/?symbol=A/RES/2450(XXIII)&Lang=S&Area=RESOLUTION

Asociación Bancaria y de Entidades Financieras de Colombia. (s.f.). *Quienes somos*. Recuperado el 20 de agosto de 2017, de https://www.asobancaria.com/quienes-somos/

Banco Mundial. (2020). *Acceso a la electricidad (% de población)*. Obtenido de Base de datos de Energía Sostenible para Todos: https://datos.bancomundial.org/indicator/EG.ELC.ACCS.ZS

Banco Mundial. (2020). *Personas que usan Internet (% de la población)*. Obtenido de Informe sobre el Desarrollo Mundial de las Telecomunicaciones/TIC y base de datos.: https://datos.bancomundial.org/indicador/IT.NET.USER.ZS

Barranco Fragoso, R. (18 de Junio de 2012). *¿Qué es Big Data?* Obtenido de IBM Developer Works: https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/

Becarés, B. (12 de Enero de 2017). *7 tendencias del Big Data, según Tinámica*. Obtenido de http://www.siliconweek.com: http://www.siliconweek.com/data-storage/bigdata/7-tendencias-del-big-data-segun-tinamica-74065#8wRRTZmZAqxD1gL7.99?inf_by=595ff79e671db8b0298b48dd

Bejarano, M. R. (Enero de 2014). *Evolución del derecho de protección de datos personales en Colombia respecto estándares internacionales.* Obtenido de Editorial Universidad Católica: http://editorial.ucatolica.edu.co/ojsucatolica/revistas_ucatolica/index.php/Juridica/article/viewFile/652/670

Berman, D. (2017). *Global Guide to Data Protection Laws.* CipherCloud.

Berman, H. J. (s.f.). *La Formación de la Tradición Jurídica de Occidente.* México: Fondo de Cultura Económica.

Berman, J. J. (2013). *Principles of Big Data : Preparing, Sharing, and Analyzing Complex Information.* Amsterdam: Morgan Kaufmann.

Casey, A. (. (1 de Septiembre de 2016). *"Focus feature: Artificial intelligence, big data, and the future of law."* . Obtenido de University Of Toronto Law Journal 66, no. 4: http://eds.a.ebscohost.com.ez.urosario.edu.co/eds/pdfviewer/pdfviewer?vid=8&sid=632acad7-c63b-4c7f-8c96-c4f15df3685c%40sessionmgr4008

Castells, M. (2006). *La era de la información: Economía, sociedad y cultura.* Cambridge: Siglo XXI editores, s.a.

Castro Rueda, C. (2015). *Desde los lados del Atlántico: Big Data y una mirada a los modelos normativos europeo y estadounidense sobre la protección de datos personales.* Bogotá: Trabajo de Grado para obtener el Título de Abogada, Universidad de los Andes.

Centro de Excelencia y Apropiación en Big Data y Data Analytics. (s.f.). Obtenido de Alianza Caoba: http://alianzacaoba.co/

Chaves, J. (2004). Desarrollo Tecnológico en la Primera Revolución Industrial. *Norba. Revista de Historia, 17*, 93-109.

Cifuentes Muñoz, E. (1997). El habeas data en Colombia. *Revista de la Facultad de Derecho PUCP*(51), 115-144. Obtenido de http://revistas.pucp.edu.pe/index.php/derechopucp/article/view/6106/6112

Cloud Servers. (s.f.). Obtenido de Data Center Map: https://www.datacentermap.com/cloud.html

CONPES, Consejo Nacional de Política Economica y Social. (17 de Abril de 2018). *Política Nacional de Explotación de Datos Documento 3920.* Obtenido de Departamento Nacional de Planeación: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3920.pdf

Constitución Politica. (20 de Julio de 1991). Colombia.

Davis, N. (19 de Enero de 2016). *What is the fourth industrial revolution?* Obtenido de Foro Económico Mundial: https://www.weforum.org/agenda/2016/01/what-is-the-fourth-industrial-revolution/

Decreto 1377. (27 de Junio de 2013). *Decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.* Colombia. Obtenido de Decreto por el cual se reglamenta parcialmente la Ley 1581 de 2012.: https://www.sic.gov.co/sites/default/files/normatividad/DECRETO%2B1377%2BDEL%2B27%2BDE%2BJUNIO%2BDE%2B2013.pdf

Decreto 1727. (15 de Mayo de 2009). *Decreto por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.* Colombia. Obtenido de https://www.sic.gov.co/sites/default/files/normatividad/Decreto_1727_2009%20pdf.pdf

Decreto 2591. (19 de Noviembre de 1991). *Por el cual se reglamenta la acción de tutela consagrada en el artículo 86 de la Constitución Política*. Colombia.

Decreto 2952. (6 de Agosto de 2010). *Decreto por el cual se reglamentan los artículos 12 y 13 de la ley 1266 de 2008*. Colombia. Obtenido de https://www.sic.gov.co/sites/default/files/normatividad/Decreto_2952_2010.pdf

Decreto 886. (13 de Mayo de 2014). *Decreto por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos*. Colombia. Obtenido de https://www.sic.gov.co/sites/default/files/normatividad/Decreto_886_2014.pdf

Dirección Nacional de Planeación - DNP-. (22 de Marzo de 2016). *Big Data: Colombia entra en la revolución de los datos*. Obtenido de Dirección Nacional de Planeación - DNP-: https://www.dnp.gov.co/Paginas/Big-Data-Colombia-entra-en-la-revoluci%C3%B3n-de-los-datos-.aspx

DW Documental. (10 de Mayo de 2019). Amazon, Jeff Bezos y la colección de datos. Obtenido de https://www.youtube.com/watch?v=UzGemfwaTT8

Echavarría, J., Villamizar, M., & González, J. (s.f.). *El Proceso Colombiano de Desindustrialización.* Obtenido de Banco de la República de Colombia: https://www.banrep.gov.co/docum/ftp/borra361.pdf

EFE / 20MINUTOS. (7 de Julio de 2013). *Cronología del 'caso Snowden', el joven que reveló el espionaje masivo de Estados Unidos*. Obtenido de https://www.20minutos.es: https://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/#xtor=AD-15&xts=467263

Ekstrand, V. S. (2015). *Hot News in the Age of Big Data: a Legal History of the Hot News Doctrine and Implications for the Digital Age.* eBook Collection (EBSCOhost): El Paso: LFB Scholarly Publishing LLC.

El Tiempo. (27 de Octubre de 2008). *Hitos tecnológicos en el país*. Obtenido de Periodico El Tiempo: https://www.eltiempo.com/archivo/documento/MAM-3158698

Foro Económico Internacional. (s.f.). *Historia: Foro Económico Internacional*. Obtenido de Foro Económico Internacional: https://www.weforum.org/about/history

Gonçalves, M. E. (2017). The EU data protection reform and the challenges. *Information & Communications Technology Law*, VOL. 26, NO. 2, 90–115.

Google Spain, S.L., y Google Inc. Vs. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González,, C-131/12 (Tribunal de Justicia Europeo 13 de Mayo de 2014).

Grupo Banco Mundial. (s.f.). *China*. Obtenido de https://www.bancomundial.org/: https://datos.bancomundial.org/pais/china?view=chart

Hernández, G. (2011). *HISTORIA DE LAS COMPUTADORAS.* Obtenido de Universidad Veracruzana: https://www.uv.mx/personal/gerhernandez/files/2011/04/historia-compuesta.pdf

hipertextual.com. (2 de Diciembre de 2016). *El papel de la cuarta revolución industrial en la economía mundial*. Obtenido de hipertextual.com: https://hipertextual.com/presentado-por/dell-emc/cuarta-revolucion-industrial-dell

Historia de la base de datos: evolución, gestores y mas. (s.f.). Recuperado el 15 de Abril de 2020, de Conoce la historia: https://conocelahistoria.com/c-tecnologia/historia-de-la-base-de-datos/

Lane, M. (23 de Abril de 2012). *¿Cómo se entera una tienda antes que tus padres de que estás embarazada?* Obtenido de CNN en español: http://cnnespanol.cnn.com/2012/04/23/como-se-entera-una-tienda-antes-que-tus-padres-de-que-estas-embarazada/

Leuan Jolly, L. &. (1 de Julio de 2017). *Data protection in the United States: overview*. Obtenido de Thomson Reuthers: Practical Law: https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

Ley 1266. (31 de Diciembre de 2008). *Ley Estatutaria de habeas data financiero*. Colombia.

Ley 1581. (11 de Octubre de 2011). *Ley Estatutaria de protección de datos personales*. Colombia.

Ley 1712. (6 de Marzo de 2014). *Ley de Transparencia y del Derecho de Acceso a la Información Pública*. Colombia.

Losano, M. G. (1989). El Anteproyecto de ley colombiana de 1987. En M. G. Losano, A. E. Pérez Luño, & M. F. Guerrero Mateus, *21 Cuadernos y debates: Libertad informática y leyes de protección de datos personales* (págs. 95-99). Madrid, España: Centro de Estudios Constitucionales.

Martin, A. (6 de Octubre de 2015). *¿Qué es el Safe Harbor y qué implica su anulación para los ciudadanos de la UE?* Obtenido de Hipertextual.com: https://hipertextual.com/2015/10/anulacion-safe-harbor

MasterFILE Premier. (28 de Noviembre de 2016). *"Data for the People: How to Make Our Post-Privacy Economy Work for You."*. Obtenido de Publishers Weekly 263, no. 48: http://eds.a.ebscohost.com.ez.urosario.edu.co/eds/detail/detail?vid=3&sid=632acad7-c63b-4c7f-8c96-c4f15df3685c%40sessionmgr4008&bdata=Jmxhbmc9ZXM%3d#AN=119714837&db=f5h

Merino, P. P. (18 de Mayo de 2016). *Los datos, el nuevo petróleo del siglo XXI*. Obtenido de Ecommerce News: http://ecommerce-news.es/actualidad/los-datos-nuevo-petroleo-del-siglo-xxi-41824.html#

Montezuma Chavez, D. F. (2019). *La responsabilidad demostrada frente al tratamiento de datos personales y su relevancia para la graduación de la sanción al interior de procedimientos administrativos sancionatorios.* Obtenido de Trabajo de grado para obtener el título de Magíster en Derecho Administrativo. Pontificia Universidad Javeriana: https://repository.javeriana.edu.co/handle/10554/47748

Newman Pont, V., & Ángel Arango, M. P. (Enero de 2019). *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital.* Obtenido de Dejusticia, centro de estudios jurídicos y sociales.:

https://cdn.dejusticia.org/wp-content/uploads/2019/01/Rendicio%CC%81n-de-cuentas-de-Google-y-otros-negocios-en-Colombia.pdf

Ning, S., & Wu, H. (7 de Junio de 2020). *China: Data protection laws and regulations 2020*. Obtenido de ICGL.com: https://iclg.com/practice-areas/data-protection-laws-and-regulations/china

OCDE. (23 de Septiembre de 1980). *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales.* Obtenido de http://www.oecd.org: http://www.oecd.org/sti/ieconomy/15590267.pdf

Oficina de Estudios Económicos, Mincit. (21 de Diciembre de 2020). *Perfil de China*. Obtenido de Ministerio de Industria, Comercio y Turismo de Colombia: https://www.mincit.gov.co/getattachment/estudios-economicos/perfiles-economicos-y-comerciales/en-este-espacio-encontrara-los-perfiles-economicos/asia/asia-del-este/china/oee-espanol-perfil-china-21-12-2020.pdf.aspx

Olano, H. (2019). Historia de la regeneración constitucional de 1886. *Revista IUS*.

Oracle Colombia. (s.f.). *Definición de big data*. Obtenido de Oracle Colombia: https://www.oracle.com/co/big-data/what-is-big-data/

Parra, S. (30 de Marzo de 2015). *La herramienta de Facebook para combatir la depresión*. Obtenido de Xatakaciencia: https://www.xatakaciencia.com/salud/la-herramienta-de-facebook-para-combatir-la-depresion

Peirano, M. (22 de Septiembre de 2015). *¿Por qué me vigilan, si no soy nadie?* Obtenido de TEDxMadrid Youtube: https://www.youtube.com/watch?v=NPE7i8wuupk

Peralta, J. A. (s.f.). *La maravillosa invención de la pila de Volta.* Obtenido de Departamento de Fisica, ESFM-IPN:

https://www.esfm.ipn.mx/assets/files/esfm/docs/RNAFM/articulos-2021/XXVIRNAFM003.pdf

Preguntas Frecuentes. (s.f.). Obtenido de Privacidad y Condiciones: https://www.google.com/intl/es/policies/faq/

Press, G. (9 de Mayo de 2013). *A Very Short History Of Big Data*. Obtenido de Revista Forbes: https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/#a08167665a18

Proyecto de ley estatutaria número 27. (25 de Julio de 2006). *Gaceta del Congreso 246*, págs. 11-18. Obtenido de http://svrpubindc.imprenta.gov.co/senado/index2.xhtml?ent=Senado&fec=25-07-2006&num=246

Quinn, J. (2017). A Peek over the Great Firewall: A Breakdown of China's New Cybersecurity Law. *SMU Science and Technology Law Review*, 407–436. Obtenido de https://heinonline-org.ez.urosario.edu.co/HOL/Page?handle=hein.journals/comlrtj20&div=28

Red Iberoamericana de Protección de Datos (RIPD). (s.f.). *Relación de entidades integrantes de la RIPD*. Obtenido de Red Iberoamericana de Protección de Datos (RIPD): https://www.redipd.org/es/la-red/entidades-acreditadas

Red Iberoamericana de Protección de Datos. (s.f.). *Historia de la Red Iberoamericana de Protección de Datos*. Obtenido de https://www.redipd.org/es: https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd

Remolina Angarita, N. (1994). El habeas data en Colombia. *Revista de Derecho Privado de la Universidad de los Andes*, 185-225. Obtenido de Observatorio Ciro Angarita Baron sobre la protección de datos personales en Colombia: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/El-habeas-data-en-Colombia-1994-R15_A4.pdf

Remolina, N. (2013). *Tratamiento de Datos Personales. aproximación internacional y comentarios a la Ley 1581 de 2012*. Bogotá: LEGIS.

Revista Dinero. (7 de Agosto de 2015). *Big Data: la mina de oro*. Obtenido de Revista Dinero Sección Tecnología: http://www.dinero.com/edicion-impresa/tecnologia/articulo/el-poder-economico-del-big-data-su-desarrollo-colombia/210853

Revista Semana. (s.f.). *Marzo 3 de 1957 La máquina que cambió al país*. Obtenido de Revista Semana: https://www.semana.com/especiales/articulo/marzo-1957-brla-maquina-cambio-pais/65917-3/

Rodríguez Soler, A. (2020). El «big data» y su papel en la construcción de Historias: una mirada de las Ciencias Sociales. *Serie Científica de la Universidad de las Ciencias Informáticas, 13*(5), 16-24. Recuperado el 10 de Julio de 2021

Sadurní, N. (19 de Febrero de 2021). *Alan turing, el arma secreta de los aliados*. Obtenido de Historia, National Geographic: https://historia.nationalgeographic.com.es/a/alan-turing-arma-secreta-aliados_16352

SAS Colombia . (21 de Diciembre de 2016). *El crecimiento y transformación de las compañías del siglo XXI depende de la correcta interpretación de sus datos*. Obtenido de SAS Latin America : http://blogs.sas.com/content/sasla/2016/12/21/el-crecimiento-y-transformacion-de-las-companias-del-siglo-xxi-depende-de-la-correcta-interpretacion-de-sus-datos/

Schwab, K. (14 de Enero de 2016). *The Fourth Industrial Revolution: what it means, how to respond*. Obtenido de Foro Económico Mundial: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

Secretaría de Asuntos Jurídicos. (3 de Enero de 2022). *Principios actualizados sobre la privacidad y la protección de datos personales.* Obtenido de Organización de los Estados Americanos: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

Senso, J. A., & De la Rosa Piñero, A. (Mayo/Agosto de 2003). El concepto de metadato. Algo más que descripción de recursos electrónicos. *Scielo , 32*(2), 95-106. Obtenido de Scielo: http://www.scielo.br/pdf/ci/v32n2/17038.pdf

Sentencia C-1011, C-1011 (Corte Constitucional de Colombia 16 de Octubre de 2008).

Sentencia C-748, C-748 (Corte Constitucional de Colombia 6 de Octubre de 2011).

Sentencia SU-082, SU-082 (Corte Constitucional de Colombia 1 de Marzo de 1995).

Sentencia SU-458, SU-458 (Corte Constitucional de Colombia 21 de Junio de 2012).

Sentencia T 414, T 414 (Corte Constiucional 16 de Junio de 1992).

Sentencia T-414, T-414 (Corte Constitucional de Colombia 16 de Junio de 1992).

Sentencia T-729, T-729 (Corte Constitucional de Colombia 5 de Septiembre de 2002).

Sentencia T-964, T-964 (Corte Constitucional de Colombia 29 de Noviembre de 2010).

Snowden, E. (2016). *I AM Edward Snowden, Ask Me Anything.* . Obtenido de Reddit: https://np.reddit.com/r/technology/comments/4cvhi0/i_am_edward_snowden_ask_me_anything/d1lpmtq/?context=3

Statista. (2018). *Previsión de los ingresos de la industria de big data en el mundo entre 2016 y 2027 (en miles de millones de dólares)*. Recuperado el 10 de Junio de 2018, de https://es.statista.com/estadisticas/517644/prevision-del-valor-de-mercado-del-big-data-en-el-mundo/

Superintendencia de Industria y Comercio. (2015). *Guía para la Implementación del Principio de Responsabilidad Demostrada (accountability)*. Colombia. Obtenido de https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Superintendencia de Industria y Comercio. (2019). *Guía para la Implementación del Principio de Responsabilidad Demostrada en las Transferencias Internacionales de Datos Personales*. Colombia. Obtenido de https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales(1).pdf

Superintendencia de Industria y Comercio. (29 de Mayo de 2020). *Circular Única*. Recuperado el 17 de Agosto de 2020, de Web Oficial Superintendencia de Industria y Comercio: https://www.sic.gov.co/sites/default/files/normatividad/052020/Ti%CC%81tulo%20V%20Proteccion%20Datos%20Circular%2003%20del%2030%20de%20marzo%202020%29.pdf

Superintendencia de Industria y Comercio. (20 de Enero de 2020). *Día Internacional de Protección de Datos: un llamado a las buenas prácticas*. Obtenido de https://www.sic.gov.co/noticias: https://www.sic.gov.co/noticias/d%C3%ADa-

internacional-de-protecci%C3%B3n-de-datos-un-llamado-las-buenas-pr%C3%A1cticas

Superintendencia de Industria y Comercio. (28 de Enero de 2022). *Más de 28 mil quejas recibió la Superindustria en 2021 por protección de datos personales*. Obtenido de https://www.sic.gov.co/slider/m%C3%A1s-de-28-mil-quejas-recibi%C3%B3-la-superindustria-en-2021-por-protecci%C3%B3n-de-datos-personales#:~:text=BALANCE%20DE%20GESTI%C3%93N%20EN%20PROTECCI%C3%93N,recibidas%20durante%20el%20a%C3%B1o%202020.

Superintendencia de Industria y Comercio. (s.f.). *Registro Nacional de Bases de Datos*. Recuperado el 11 de Agosto de 2019, de http://www.sic.gov.co/registro-nacional-de-bases-de-datos

Tecnósfera. (27 de Octubre de 2017). *Como en Black Mirror, China califica a sus ciudadanos*. Obtenido de Tecnología Periodico El Tiempo: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/sistema-de-calificacion-a-ciudadanos-en-china-145486

The Guardian. (6 de Junio de 2013). *Verizon forced to hand over telephone data – full court ruling*. Obtenido de https://www.theguardian.com: https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order

Unión Internacional de Telecomunicaciones. (s.f.). *Informe sobre el Desarrollo Mundial de las Telecomunicaciones/TIC y base de datos.* Obtenido de Banco Mundial: https://datos.bancomundial.org/indicator/IT.NET.USER.ZS

Valbuena Abogados. (9 de Marzo de 2017). *Estudio sobre la aplicación en Colombia de las normas sobre transferencia internacional de datos personales.* Obtenido de

Superintendencia de Industria y Comercio: http://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/consulta_avanzada/TRANSFERENCIA-INTERNACIONAL-DE-DATOS-PERSONALES-09-03-2017.pdf

Valencia, D. (2015). *El Estado en la Era de la Globalización y las Nuevas Tecnologías.* Bogotá: Grupo Editorial Ibañez.

Weigend, A. (2016). *DATA FOR THE PEOPLE.* Basic Books. Obtenido de http://www.weigend.com/

Yin, K., & Zhang, G. (26 de Octubre de 2020). *A look at China's draft of Personal Information Protection Law*. Obtenido de The International Association of Privacy Professionals: https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/

Zhang, L. L. (15 de Marzo de 2020). *Does Huawei React Well to the US Sanction in the Aspect of Finance?* Obtenido de ideas-repec-org.: https://ideas-repec-org.ez.urosario.edu.co/p/osf/thesis/82ne3.html

Zuboff, S. (2019). *The age of surveillance capitalism : the fight for a human future at the new frontier of power.* New York: PublicAffairs.