LA PROTECCION DE DATOS EN LA ERA DIGITAL COLOMBIA - ESPAÑA

Data protection in the digital era
Colombia – Spain

Jhony Ariza Herrera.
joarizah@poligran.edu.co

Jorge Eliécer Ayala Fandiño.
joayalaf@poligran.edu.co

Luis Eduardo González de la Zerda.
lagonzalez27 @poligran.edu.co

Institución Universitaria Politécnico Grancolombiano
Derecho
Colombia

Resumen

El presente artículo es resultado de un método de investigación teórica con un enfoque cualitativo-inductivo, en este se pretende describir el sistema colombiano y español en relación con la protección de datos, esto a fin de dilucidar sobre los aspectos de mayor relevancia en la normativa. Se iniciara analizando los aspectos conceptuales del tratamiento de datos al igual que se precisa sobre algunos principios que resultan importantes a la hora de tratar los datos personales, acto seguido se analiza sobre el desarrollo tecnológico y las implicaciones que esta ha tenido en el tratamiento de los datos, haciendo notar los retos que debe afrontar el legislador en el marco de las nuevas tecnologías, continuando con una análisis del sistema normativo colombiano dende se revelan aspectos generales de la protección de datos en este país, así mismo se realizan algunas apreciaciones sobre su control y tratamiento, y por último se analiza el sistema normativo español haciendo a grandes rasgos un recorrido histórico de la normativa de este país y dejando en evidencia los avances frente al tratamiento de datos y garantías digitales que se crean al tenor de la Ley orgánica 03/2018.

Summary

This articule is the result of a theoretical research method with a qualitative-inductive approach, in which it is intended to describe the Colombian and Spanish system in relation to data protection, this in order to elucidate the aspects of greater relevance in the regulations. In developing this, it begins by analyzing the conceptual aspects of data processing as well as specifying some principles that are important when treating personal data, then it is analyzed on the technological development and the implications that this has had on data treatment, noting the challenges that the legislator must face in the framework of new technologies, continuing with an analysis of the Colombian regulatory system where general aspects of data protection in this country are revealed, as well as some appraisals on its control and treatment, and finally the Spanish regulatory system is analyzed by making a broad overview of the history of the regulations of this country and highlighting the advances in the treatment of data and digital guarantees that are created in accordance with the Organic Law 03/2018.

Palabras clave:

Nuevas tecnologías, tratamiento de datos, España, Colombia, normativa.

Keywords:

New technologies, data processing, Spain, Colombia, regulations.

Recepción: **Aceptación:**

Cite este artículo como: Ayala, J., Ariza, J. y González, L. (2020). La protección de datos en la era digital Colombia - España. Revista Politécnico Grancolombiano. Bogotá, Colombia.

Introducción

En la actualidad con más frecuencia se hace notoria la propagación de nuevos medios de información y comunicación por los cuales se divulgan datos de diverso contenido, allí se pueden apreciar los datos personales de cada sujeto, estas grandes fuentes de información son conocidas como Nuevas tecnologías de la información y comunicación en adelante (NTIC), las cuales con frecuencia son utilizadas por las personas para abrir la puerta a una nueva manera de divulgación masiva de información, esto en diferentes área por ejemplo en la construcción del conocimiento, el trabajo, en el ámbito social, entre otros, de los cuales se evidencia como resultado el cambio de las dinámicas de interacción entre personas.

Estas tecnologías (NTIC) presentan una notoria incidencia en las relaciones sociales, culturales, económicas, entre otras, estas a su vez pueden ser el origen de una variedad de relaciones jurídicas que han llevado a que se deba analizar desde el derecho este fenómeno. Todo este movimiento de nuevas posibilidades ha generado que el legislador se vea en la tarea de remover aquellos baches que dificultan el disfrute de los beneficios de estas nuevas herramientas, pero de igual manera se ve en la obligación blindar las relaciones jurídicas que allí se presentan, de todos los inconvenientes que esta puede traer consigo, a fin de garantizar una estabilidad social y seguridad jurídica (Peguera et al, 2004, p. 13).

Los ordenadores junto con otros medios tecnológicos son las herramientas que impulsan todo este movimiento, haciendo posible la divulgación a dimensiones globales, generando así reflexiones frente a cómo deben ser abordadas las libertades y garantías individuales tales como la privacidad e intimidad personal (Muñoz, s.f.). Las nuevas herramientas digitales han causado la transformación del tratamiento que se le da a los datos, anteriormente se solicitaba información personal básica y con ello se realizaba un análisis para cumplir con los fines para los cuales era solicitada; en la actualidad existe un tratamiento de datos más veloz dónde se van generando datos en vez de simplemente recolectarlos, esto como muestra del avance ya mencionado (Recio, 2019, p. 14).

Existen algunos principios los cuales resultan fundamentales para que el tratamiento de los datos personales cuente con legalidad en todos los escenarios digitales, por un lado debe existir el principio de información, mediante este se pretende que quién suministra los datos tenga conocimiento del manejo que se le dará a los mismos por parte de quién los esté requiriendo; por otro lado se encuentra el principio de finalidad del tratamiento, lo que esto quiere decir es que el uso que se le dé a los datos debe tener propósitos legítimos y claros. Por último, se encuentra el principio de minimización de datos, este consiste en que los datos que vayan a ser requeridos sean los necesarios para el fin que se pretende, es decir, que no sea solicitada información adicional a la pertinente (Recio, 2019, pp. 24-25).

Frente al tratamiento de datos, organismos internacionales se han pronunciado al respecto, mencionando la importancia de que existan diversos principios los cuales coadyuven con la normativa existente para así generar una mayor garantía en dicha protección, un ejemplo de ello es que por medio de una resolución de la Asamblea General de las Naciones Unidas se establecieron algunos principios como marco del tratamiento de datos personales, por su parte, la Organización para la Cooperación y Desarrollo Económico (OCDE), ofreció algunas recomendaciones que mencionan también principios a tener en cuenta con el

fin de salvaguardar la seguridad de los datos personales (Recio, 2019, p. 15).

A la orden de estos principios y como interés del presente artículo, es preciso advertir que frente a esto, Colombia reconoce dentro de su normativa la necesidad de tener figuras que tutelen garantías tales como la intimidad y la información personal, consagrados en el artículo 15 de la Constitución Política, dónde es mencionado el derecho con el que toda persona cuenta de que la información que suministra posee unos lineamientos de seguridad, existiendo así previa autorización del titular de los datos para que los mismos circulen o sean utilizados, y permitiendo a su vez que en caso de que exista un mal manejo de dichos datos, puedan llevarse a cabo las respectivas acciones legales.

Al tratar el tema de protección de datos nos encontramos frente a un mandato legal el cual dentro del sistema jurídico colombiano halla su principal sustento en la Ley 1581 de 2012 donde se regula dicha salvaguarda de datos desde su recolección hasta su transmisión, exigiendo así que el tratamiento de la información recibida cumpla con los parámetros necesarios para garantizar la protección integral de los mismos (Botero y Martín, 2016, pp. 5-10).

A fin de contrastar el manejo de datos del sistema colombiano resulta pertinente traer a colación el sistema español, pues llama la atención que este cuenta con una regulación normativa que procura cubrir integralmente la garantía constitucional de la intimidad, esto respecto al tratamiento de datos que se da en ámbitos laborales, judiciales, de administración pública, entre otros. Lo que esto quiere decir es que España cuenta con un sistema de protección de datos el cual procura salvaguardar la mayor parte de los campos en los cuáles puede verse inmersa e involucrada la información personal, pretendiendo garantizar de esta manera el adecuado manejo de los datos y evitando que se configuren eventos ilícitos.

El presente artículo pretende realizar una comparación entre el sistema normativo colombiano y español referente a la protección de los datos personales frente a las (NTIC), procurando de esta manera analizar la pertinencia de cubrir plenamente el tratamiento de datos, teniendo en cuenta que es España el país pionero en el reconocimiento del derecho fundamental consistente en que los datos personales cuente con una protección, garantizando a toda persona la existencia de un control legitimo sobre los datos que proporciona.


Designed by Freepik

Método

El presente artículo consta de un enfoque cualitativo en el marco de una investigación teórica que se afinca a la conjetura que pretendemos desarrollar, al encontrar útil incursionar y contrastar sistemas normativos en referencia a los datos personales, para tal fin el presente artículo pretende hacer un comparativo entre el sistema normativo colombiano y el sistema español. La presente investigación es documental y permite una dinámica entre los hechos y la interpretación que se le da a los mismos, de igual manera

posibilita condensar aforismos, conceptos y postulados que son extraídos mediante fuentes bibliográficas tales como, libros, artículos, ensayos, códigos, entre otras. En desarrollo transversal el presente trabajo cuenta con un método deductivo haciendo un análisis desde las generalidades a situaciones específicas sistematizando conocimiento y estableciendo inferencias que permiten ser analizadas desde diferentes perspectivas (Villabella, 2015, p. 6).

Designed by Freepik

Resultados

1. Tratamiento de datos: un recorrido conceptual.

Los datos personales continuamente son captados por entidades, así mismo deben ser administrados por estas y en ocasiones son objeto de divulgación, en razón a esto se ha visto en diferentes legislaciones como un derecho fundamental que debe ser protegido, por tal motivo su tratamiento debe responder a los principios que permitan un buen manejo de estos, lo que se traduce en utilizar los datos para los fines solicitados, ser obtenidos y manejados solo por personas autorizadas. Para tal efecto la protección de datos puede ser entendida como aquel apartado legal que se encarga de proteger el derecho fundamental de la intimidad personal en relación con el tratamiento como lo es la captación, administración y divulgación (García. 2007, p. 11).

Aquellos fenómenos que impulsan los nuevos cambios sociales, como lo es la tecnología, son los que hacen que el legislador se vea en la obligación de adaptarse a las necesidades que en consecuencia son generadas; la dinámica de la protección de datos al igual que muchas otras cosas también muta, haciendo adaptaciones tanto en el ámbito público como privado.

Ahora bien, este impulso se ha visto reflejado en una ámbito internacional, pues en diversos tratados y convenios tales como la Declaración Universal de Derechos Humanos, Pacto Internacional de Derechos Civiles y Políticos, Convención Americana sobre Derechos Humanos, Convenio para la Protección de los Derechos y Libertades Fundamentales, entre otros, se hace notoria la preocupación en cuanto a la intimidad de las personas así como la protección de sus datos personales y que estos no sean objeto de posibles amenazas (Maqueo et al, 2017, p. 12).

Una vez establecido lo anterior y para abarcar el tema de la protección de datos, resulta fundamental comprender la clasificación de los datos como tal, y los diferentes factores que influyen en el concepto, pues de allí deriva que los diferentes países le den una determinada protección. El concepto de “dato personal”, corresponde a toda aquella información la cual hace posible que se identifique o reconozca determinada persona, dando claridad frente a su identificación y otros aspectos relevantes de sus circunstancias generales.

Los datos a grandes rasgos pueden clasificarse en: datos personales, datos públicos, datos semiprivados y datos

sensibles. Los datos personales son aquellos cuya información identifica a una persona natural; a su vez estos datos personales pueden ser públicos, semiprivados o privados (Rojas, 2017, p. 7). Los datos públicos son aquellos cuya información reposa en documentos de carácter público y los relacionados con el estado civil de las personas.

Los datos semiprivados, por su parte, son aquellos que resultan carecer de una naturaleza reservada, y cuya divulgación resulta interesar a algún sector, por ejemplo, respecto a lo relacionado con información financiera del individuo. Lo anterior no quiere decir que no exista ningún tipo de limitación frente a su obtención, puesto que esta sólo puede ser recibida y obtenida por las respectivas entidades competentes; por su parte, los datos privados son aquellos de carácter reservado en tanto que allí reposa información personal como lo es el domicilio, patrimonio, trayectoria profesional entre otros, razón por la cual el respectivo titular cuenta con el derecho de tener un control frente a los mismos (Almagro, 2019, p. 12).

La importancia de la clasificación mencionada con antelación responde a que el control de dichos datos va a tener un tratamiento especial dependiendo del grupo al que pertenezca y el manejo que las entidades le dan a los mismos. Es por ello que dentro de dicha clasificación fueron mencionados los llamados “datos sensibles”, los cuales están directamente relacionados con aquella información de la persona la cual tiene una afectación directa en su intimidad, como lo puede ser su ideología política, filosófica, sus creencias religiosas, entre otras.

Una vez establecida la clasificación de los datos, resulta pertinente abordar los principios que regirán la misma. Por un lado, debe existir una precaución frente a los datos que están siendo almacenados y su divulgación, observando de manera integral la existencia de medidas mediante las cuales la transparencia y el procedimiento en sí, garantice que la información que está siendo proporcionada no se verá de alguna manera comprometida en un sentido negativo.

El contenido de los datos es el motivo de otro principio fundamental, ello en razón a que el tipo de información que sea obtenido debe contar con una clasificación en la cual el factor de riesgo esté presente, ello independientemente de la forma como la información haya sido registrada, es decir, bien sea por medios tecnológicos o físicos. Esto tiene relación directa con el llamado “enfoque de gestión de riesgos”, principio por medio del cual debe ser ofrecida la protección de los datos, atendiendo así a la respectiva salvaguarda de los ya mencionados “datos sensibles”.

En continuidad con ello, se encuentra el principio de proporcionalidad relacionado con la clasificación que se da a la información recibida y su pertinencia en la ubicación dada. En congruencia con ello, el siguiente principio corresponde a la claridad que debe existir en los temas de responsabilidad, es decir, que los procesos que se estén llevando a cabo frente a los datos cuenten con un enfoque de seguridad dónde exista claridad del manejo que se adelanta. (Suarez. F et al, 2013, p. 13)

Por último y no menos importante, se encuentra el ciclo de vida de la información, y es que, en todo el proceso de gestión, debe tenerse presente que los datos pasan por diferentes fases que van desde el momento en el que son recibidos hasta que son destruidos, es por ello que es un principio por medio del cual se pretende que no exista un desconocimiento procedimental a la hora de su manejo.

Como interés del presente artículo se encuentra el manejo que se da a estos datos atendiendo a las nuevas tecnologías, pues bien, frente a ello y una vez aclarada la clasificación, es preciso mencionar que con el avance tecnológico no podían apartarse diversas consideraciones al respecto. Para procurar cubrir con la mayor cantidad de aspectos posibles, se abordó un enfoque basado en el riesgo, dónde las diferentes interacciones virtuales en las cuales se estuviese en presencia de datos personales debían pasar por un seguimiento, realizando constantemente actualizaciones de las posibles formas en las cuales se podía dar una vulneración a la protección de los datos que reposaban en las diferentes plataformas, y así mismo su posible tratamiento. (Almagro, 2019, p. 7).

En atención a ello, los datos no sólo cuentan con un respaldo de actualizaciones constantes sino con un control supervisado, lo que esto quiere decir es que, atendiendo al factor tecnológico, no es suficiente con un estudio de los posibles riesgos virtuales; pues si bien resulta ser un aspecto de gran relevancia, no logra abarcar la totalidad de implicaciones que lleva consigo el constante movimiento de datos vía web. En razón a ello, a nivel mundial existen diversas entidades las cuales coadyuvan en todas las implicaciones frente al recorrido que tienen los datos.

Como se evidencia, son diversos los factores que deben tenerse en cuenta e incluirse como respuesta a las exigencias que la tecnología trae consigo, es por ello que, sumado a lo ya mencionado, se llevan a cabo unos ajustes periódicos mediante los cuales la clasificación de los datos recibe un análisis, verificando así que los mismos se encuentren correctamente ubicados, y procurando así que no se genere un almacenaje inservible.

Designed by Freepik

2. Nuevas tecnologías y su comportamiento frente al manejo de datos

El desarrollo de la humanidad se ha visto influenciado por avances tecnológicos que siempre traen consigo aspectos novedosos, tanto positivos como negativos, por tal motivo la sociedad se ha visto en la necesidad de adaptarse a esos cambios y sacar el mejor provecho de estas situaciones, que a fin de cuenta son a las que el ser humano debe adaptarse para seguir escalando peldaños en su desarrollo.

Ahora bien, el tema que nos atañe en ocasión al presente artículo son las denominadas nuevas tecnologías de la información y la comunicación, de las cuales no se les ha podido otorgar una definición unificada, pero que a grandes rasgos podemos hablar de ellas como aquellos sistemas que ayudan a administrar y mutar la información, las cuales se desarrollan mediante el uso de herramientas como los ordenadores y programas que ayudan a crear, modificar, almacenar, proteger y recuperar la información.

Abarcando el desarrollo tecnológico y su impacto, no debe desconocerse lo que

allí se encuentra inmerso, y tema de nuestro interés, los datos personales. Estos últimos, han sido manejados desde épocas antiguas, por ejemplo, para los temas relacionados con hacienda pública los gobernantes se veían en la necesidad de realizar el debido tratamiento de los datos para entre otras cosas, verificar responsabilidades tributarias (Recio, 2019, p. 9).

Al transcurrir el tiempo, el ya mencionado desarrollo tecnológico, causó que la "simpleza" que se tenía antes frente al manejo de datos cambiara su curso, pues se evidenció la necesidad de que el manejo de los mismos llevara consigo un proceso debido, motivo por el cual las plataformas digitales se vieron en la obligación de dar la respectiva protección de datos, garantizando que los requerimientos legales quedaran resueltos.

Tanto los datos personales como las nuevas tecnologías guardan una relación directa, pues la llamada "economía digital" encuentra su sustento, por un lado, en herramientas que han permitido que se genere una facilidad en el acceso a la información, y por otro lado, en unos datos que reposan allí como resultado de largos años de expedición normativa, que a la fecha permite cubrir con gran parte de los retos que representa la diversa digitalización de actividades.

Por otro lado, el tratamiento analítico de los datos ha sido posible gracias a los sistemas tecnológicos en tanto que allí logra realizarse una clasificación de la información recibida, posibilitando el hecho de que exista mayor eficacia a la hora de su recolección y almacenamiento, y reforzando a su vez un sistema de datos seguro y optimo, por medio del cual actualmente no sólo se da dicha recolección, sino que también se da una automatización frente al procedimiento.

En ausencia de las nuevas tecnologías, la forma como se da el manejo de datos y así mismo su protección, resultaría frenada, pues no existirían las herramientas suficientes para solventar la demanda de las interacciones sociales y no sólo ello, sino la protección integral de los datos que continuamente circulan por las diferentes plataformas digitales.

En relación con lo anterior, la información que se maneja en los diferentes medios tecnológicos de almacenamiento va en constante aumento y esto se refleja notoriamente en las cifras, pues al año 2013 se concebía en una suma en unidades de almacenamiento de información de 4.4 zettabytes de información de diferente tipo rondando por plataformas digitales. Para el año 2020 se aprecia una suma bastante diferente, pues se estima un incremento considerable, perteneciente a 44 zettabytes de información rondando por las diferentes plataformas (Recio, 2019, pp. 9-10).

Este crecimiento en el manejo de información se encuentra estrechamente relacionado con los diferentes medios tecnológicos que se utilizan para hacer posible la divulgación masiva de los datos; en el año 2018 se estimaba una cantidad de 23.14 billones de dispositivos digitales que hacían uso a plataformas como internet, de esta cantidad de dispositivos llama la atención que resulta ser más elevada que la cantidad de usuarios que se registran, pues para el mismo años se estimaba un total de 3.9 billones de usuarios conectados (Recio, 2019, p. 11).

Ahora bien, estas son cifras que se encuentran en constante aumento pues se estima que para el año 2025 sean 75.44 billones de dispositivos que se encuentren conectados a internet (Recio, 2019), lo que genera que sea necesario reflexionar sobre las abrumadoras cifras de información que esto representa; si bien podrían ser datos

personales o no, se debe apreciar la manera en cómo se regularan estos cambios a fin de no generar afectaciones en las garantías fundamentales que se ponen en riesgo con el uso de las mismas.

Este crecimiento trae consigo conceptos como “IP”, estos son protocolos de interconexión que se le asignan a cada dispositivo que se conecta a internet; este consiste en códigos con unas cualidades en sus caracteres que permite identificar cada dispositivo de otro. Estos códigos tienen tendencia a ser parte de las diferentes clases de datos incluso personales, llama la atención la cantidad de usuarios que se registran en internet, pues es evidente que el constante crecimiento de estos supera la cantidad de personas que hay en el mundo, por tal motivo la tendencia puede cambiar y habrá que precisar en cada uno de estos códigos si se trata de datos personales o no.

En conjunto con lo anterior surgen nuevas tecnologías, por ejemplo, el “*blockchain”,* que se traduce como cadena de bloques, la definición de esta se asemeja a un libro contable público, unas bases de datos que son utilizadas para tener registro de transacciones copiadas por ordenadores en redes de interconexión específicas, esta tecnología puede ser medio para diversos tratamientos de datos que pueden ser personales o no. (EquiSoft, 2017, p. 12)

Es preciso advertir que este sistema de tratamiento de datos se genera por unos códigos específicos que permiten mantener al usuario en el anonimato, esto trae consigo que a pesar de que la información sea publica, no es posible que personas ajenas puedan relacionar la transacción con el titular de la misma, resguardando de alguna manera los datos.

Por su parte, conceptos como *Cloud Computing* también hacen parte de este nuevo desarrollo tecnológico que surge al margen de la cuarta revolución industrial, usándose con frecuencia una variedad de servicios de computación, que se ofrecen en operación directa de internet, este modelo no cuenta con una definición unificada; sin embargo este se puede entender como un sistema que se extiende a todas partes y que surge bajo la demanda de recursos de cómputo compartidos y automatizados, que puede rápidamente proporcionar y liberar información con un mínimo de interacción entre el usuario y el proveedor (Urueña et al, 2019, p. 3).

Continuando con conceptos de relevancia, aparece el internet de las cosas “*IoT*”, este concepto lleva consigo elementos y procesos dónde existe una “interconexión de objetos”, causando que gracias a las nuevas herramientas informáticas surjan programas que permiten el correcto funcionamiento de la comunicación, llevando consigo la posibilidad de aplicación en diferentes sectores de gran importancia.

En relación al ya mencionado desarrollo tecnológico resulta importante señalar que todos y cada uno de estos trae consigo un reto que debe ser afrontado por el legislador, pues es de reflexionar sobre la seguridad, que estas plataformas suministran a los datos y la forma como se responde normativamente a estas situaciones, al unísono se analiza la confidencialidad así como la privacidad y la integridad personal; lo que esto quiere decir es que resulta de especial análisis como se maneja el tratamiento de datos al margen de la cuarta revolución industrial y como las tecnologías que tienen influencia directa en el manejo de los datos son valoradas desde un ámbito normativo a fin de no permitir posibles afectaciones a las garantías fundamentales que se ponen en riesgo por el uso de las mismas.

Designed by Freepik

3. Protección de datos en Colombia: un recorrido normativo

Pese a una regulación desde la normativa constitucional sobre la protección de datos, podríamos advertir que Colombia es un país que ha incursionado en este tema recientemente y lo ha hecho con un desarrollo pertinente de manera paulatina a fin de garantizar la protección al derecho fundamental que consagra la Declaración Universal de Derechos Humanos en su artículo 12, donde reza que "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." (DUDH, 1948).

Este fundamento internacional sirvió como base para que en Colombia este derecho fundamental fuese incorporado dentro de su normativa. Promulgada la Constitución del 1991 se consagro formalmente dentro del artículo 15 la garantía fundamental a la intimidad personal y el buen nombre, en consecuencia, el Estado debía expedir normas que desarrollen este artículo a fin de tutelar la seguridad de los datos personales de los ciudadanos.

Como respuesta a lo anterior surge la Ley 1266 de 2008, la cual regula la utilización de datos personales referente a temas crediticios, financieros, comerciales y de servicios, lo que esto representa es que en virtud de esta ley se protege exclusivamente los datos que ostentan información que conforma el historial crediticio de los sujetos, simbolizando así la protección exclusiva de lo que se denominó *"habeas data crediticio"* (Superintendencia Industria y Comercio, s.f.).

Dentro de esta misma se fijaron directrices en las cuales se relacionaban aspectos que involucraban la recolección y la circulación de datos financieros a fin de garantizar la mayor seguridad a esta, de igual manera fueron consignados principios que contribuirían a la salvaguarda de la información tales como: la veracidad de los registros de datos, la finalidad legitima, la no circulación de los datos, la seguridad, la confidencialidad, entre otros. Por otro lado, esta ley le otorgaría al titular de la información ejercer de manera autónoma el derecho fundamental del habeas data, esto sin perjuicio de optar por algún otro medio legal.

En concordancia con lo anterior, la Corte Constitucional aclara que la administración de datos en relación con movimientos crediticios busca fines que son concurrentes a la constitución, por lo tanto, dichas entidades que administran los datos no se podrán exceder frente a sus facultades de "recolección, tratamiento y circulación" de datos personales. Por lo que resulta legitimas solo si "*(i) preservan el plexo de principios y garantías que conforman el derecho fundamental al hábeas data; y (ii) se ejercen a partir del criterio de responsabilidad social predicable de las fuentes, los operadores y*

los usuarios de la información" (M.P Dr. Jaime Córdoba Triviño Corte Constitucional, C-1011 de 2008).

Son claras las intenciones que tuvo el legislador al expedir la Ley 1266 de 2008 para tratar de regular aspectos relacionados con el manejo de datos personales, no obstante, es notorio que la misma se centró exclusivamente en el manejo de datos de carácter crediticio y financiero, en razón a esto no consigue cubrir los aspectos generales de tratamiento de datos personales, generando vacíos normativos que promovían la propagación de problemas frente al manejo de datos en entidades públicas y privadas, provocando así la necesidad de cubrir normativamente aspectos con relación al tema, a fin de incluir y salvaguardar de manera integral todo el tratamiento de datos en Colombia.

Como respuesta a la necesidad de legislar sobre aspectos generales del tratamiento de datos es expedida la Ley 1581 de 2012, mediante la cual se incorporan las disposiciones generales del almacenamiento de información, así como lineamientos en relación con la compilación, manejo y control de los datos a fin de garantizar la protección del derecho fundamental a la intimidad personal y el buen nombre en relación con manejo de la información. A grandes rasgos se puede decir que la Ley 1581 de 2012 se aplica al momento de presentarse *"recolección, almacenamiento, uso, circulación o supresión"* de datos personales que registran las entidades (Superintendencia Industria y Comercio, 2018).

La ya mencionada Ley 1581 de 2012, a diferencia de la ley de habeas data, protege integralmente cualquier clase de datos de personas jurídicas como naturales que repose en los bancos de información, en concordancia con esto las entidades de derecho público y privado quedan obligadas a proteger y fortalecer los sistemas que copilan los datos que le son confiados por los titulares de esta información (Mendoza, 2015, p. 14). Lo que esto quiere decir a la voz de la norma es que las entidades garantes de la tutela de datos personales están en la obligación de demostrar a la entidad reguladora que se implementan las medidas prudentes que garanticen el cumplimiento de los postulados que la ley establece.

A la orden de esto, se designa por disposición legal a la Superintendencia de Industria y Comercio como la entidad encargada de ejercer vigilancia con el fin de que las actividades que manejen datos personales lo hagan bajo los principios, derechos y garantías que establece la ley. De conformidad con el artículo 21 de la Ley 1581 de 2012, es función de la ya mencionada entidad: velar por el cumplimiento efectivo de esta ley, adelantar investigaciones de oficio o a petición de parte, y como consecuencia ordenar las medidas necesarias para el cumplimiento, disponer del bloqueo temporal de los datos, entre otras que garantizan el buen desarrollo y la salvaguarda del derecho fundamental a la intimidad personal y el buen nombre en relación con manejo de los datos. (Turbay, 2018, p. 16).

Es preciso advertir que la presente ley no distingue de regímenes especiales que sean analizados desde la naturaleza jurídica, lo que esto indica es que la ley tiene aplicación del manejo de los datos personales que reposen en bases de datos, sin distinguir si son entidades de derecho público o privado, aclarando que para tales efectos se entenderá el manejo de datos como *"conjuntos organizados o depósitos ordenados de datos personales sujetos a tratamiento"* (Ley 15 de 2012, art. 3).

Dentro de la misma ley se contempla una excepción al manejo de datos, llama con especial atención el artículo 10 de la Ley 1581 de 2012, pues a la voz de este se expresa que la autorización previa por el titular de la información no es solicitada en situaciones en las que la información es *"requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, cuando son datos de naturaleza pública, Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos, Datos relacionados con el Registro Civil de las Persona Casos de urgencia médica o sanitaria*"; esta disposición fue analizada por la sala plena de la Corte Constitucional realizando la aclaración pertinente en relación con estos momentos de excepción a la autorización de datos.

En el literal "a" de la misma, se menciona que no se requiere la autorización del titular cuando la Información sea "*requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial*", para tal efecto la sala de la Corte Constitucional precisa que a raíz de ello no puede generarse ningún tipo de abuso en cuanto a la información que está siendo recibida por parte de los funcionarios del Estado (*M.P Dr. Jaime Córdoba Triviño Corte* Constitucional, C-1011 de 2008). De igual manera resalta la Corte que la entidad que solicite los datos deberá probar de manera expedita que los datos se relacionan directamente con el cumplimiento de sus funciones, y para tal fin está en la obligación de garantizar la protección a los mismos, sin perjuicio de la comunicación al titular del derecho (M.P Jorge Ignacio Pretelt Chaljub Corte Constitucional, C-748 de 2011).

Ahora bien, es preciso advertir que las sanciones que trata la ley de protección de datos se aplican por parte de la Superintendencia de Industria y Comercio en virtud del artículo 23 de la misma ley, con una aplicación directa a entidades de naturaleza privada; en razón a esto, las presuntas irregularidades que lleguen a cometer las entidades de derecho público no estarán dentro de la competencia de la Superintendencia de Industria y Comercio, sin embargo esta entidad debe adelantar dicha investigación pertinente a entidades de derecho público a fin de demostrar irregularidades si es el caso, de tal modo que si estas se encuentran se deberá trasladar el expediente a las Procuraduría General de la Nación para que esta tome las medidas sancionatorias (Turbay, 2017, p. 8).

Es meritorio que dentro del ordenamiento se contemple una normativa que regule en su mayoría los aspectos generales del tratamiento de datos para garantizar el cumplimiento irrestricto de las garantías fundamentales que este tema engloba, sin embargo, esta normativa no genera mucho impacto en la manera de evitarlo, pues la responsabilidad que tiene la entidad que almacena los datos frente al titular de los mismos se ve reducida cuando no se logra apreciar la reparación a la que tendría lugar en el caso de manipular de forma irregular los datos que le son confiados (Aguilar, 2018, p. 9).

Designed by Freepik

4. Protección de datos en España: un recorrido normativo

Es de reconocer el esfuerzo que ha desarrollado el legislador entorno a la protección de datos, pues dentro del ordenamiento jurídico español al igual que otros, el manejo de datos fue considerado como derecho fundamental previendo una latente amenaza que atentaría contra los bienes jurídicos tutelados de las personas, en atención a esto y con posterioridad del reconocimiento se desarrolla un avance frente a normas que otorgan espacial tratamiento a los datos personales, a fin de salvaguardar garantías consignadas en su Constitución (STC 254/1993).

Ahora bien, es importante anotar a grandes rasgos que los datos personales no corresponden únicamente a los datos íntimos de una persona, pues el Tribunal Constitucional de España señala que para efectos de salvaguardar el derecho fundamental, estos abarcan toda la información que pueda vulnerar el interés particular del titular por parte de un tercero, para tal efecto precisa incluso que aquellos datos de conocimiento público estarán bajo disposición del titular de la información (STC 290/2000).

Adicional a los retos del legislador por cubrir el mayor número de aspectos posibles frente al tratamiento de datos, el fenómeno tecnológico y sus avances resulto un tema que debía ser añadido a los campos de regulación, no sólo por el impacto a nivel de interacciones virtuales, sino porque de allí se desprenden sectores importantes. Previendo lo anterior, los constituyentes en 1978 añadieron dicho tema al artículo 18.4 de la Constitución Española, estableciendo: *"La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".*

Es por ello qué la normatividad de protección de datos cuenta con diversas leyes que respaldan un tratamiento seguro de los mismos, España es conocido como uno de los primeros países en consolidar este derecho, al evidenciar la pertinencia de aplicar normativa que cubriese la mayor parte de aspectos posibles en cuanto al manejo que se daba a los datos.

En consecuencia, las diferentes disposiciones que se han ido desarrollando han generado que el legislador encuentre pertinente desarrollar más a profundidad la regulación de diferentes eventos en los cuales se está ante la posibilidad de que el tratamiento de datos sea vulnerado de alguna manera. El principal ejemplo de ello resulta ser la Ley Orgánica 5/1992 del 29 de octubre, la cual fue sustituida por la Ley Orgánica 15/1999 del 5 de diciembre, consistente en la automatización del tratamiento de datos personales y así mismo, la libertad de su circulación bajo los debidos parámetros de seguridad.

En congruencia con la disposición constitucional se continuó ampliando la regulación frente al tema informático, por medio de leyes tales como la Ley 25/2007, la cual comprende la regulación de los datos en cuanto a redes públicas y en general comunicaciones vía web.

De lo anterior deriva la necesidad de que se generen precisiones normativas a fin de que exista el menor número posible de vacíos legales, por ello, en la ya mencionada Ley 25/2007 de comunicaciones electrónicas, son especificados aquellos datos los cuales deben ser de restringida divulgación, es decir, se limita la libertad de su circulación y se procura evitar que derechos tales como la intimidad se vean potencialmente en riesgo. Sumado a ello, en dicha ley se menciona el plazo de la conservación de datos que de manera general cuenta con un término de 12 meses, precisiones que

resultan ser fundamentales para la existencia de una mayor claridad en el proceso de regulación.

Continuando con la normativa en cuanto a factores tecnológicos, la Ley 32/2003 del 3 de noviembre, resulta tener gran trascendencia en ello, pues abarca el tema de las telecomunicaciones, si bien esta es una ley más general, respalda y fundamenta otras disposiciones, delimitando así las diferentes condiciones que deben cumplirse en determinados eventos, como por ejemplo el manejo dado a datos para la protección civil y la defensa nacional.

La Ley 3/2018 del 5 de diciembre, resulta ser otra normativa fundamental en el tratamiento de datos, pues por medio de esta se adapta el ordenamiento español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo del 27 de abril de 2016, pretendiendo así la existencia real de una garantía a la protección de datos personales, abarcando así mismo el tratamiento que debe darse dependiendo la categoría de los datos y los derechos que de allí derivan. Dicha Ley no sólo menciona las formas como los datos resultan ser protegidos, sino que refiere también lo concerniente al encargado o responsable de tratar los datos y las dinámicas que se llevan a cabo.

Lo concerniente al tratamiento de datos requiere también atención en cuanto al manejo que se da en un sentido internacional, es por ello que la Ley mencionada con antelación cubre también este ámbito, adaptando así el Reglamento (UE) 2016/679, dónde resulta ser aceptada normativa de aplicación vinculante, logrando así que el marco jurídico cuente con un espectro más amplio, de tal manera que todos los derechos que derivan de la ley de datos sean garantizados.

Como ejemplo de lo anterior, resulta pertinente traer a colación el acogimiento del reglamento (UE) 2016/679 del Consejo y del Parlamento Europeo, con fecha 27 de abril de 2016, en este se hace mención del seguimiento y manejo que las autoridades competentes deben dar a los datos que resulten tener fines concernientes a asuntos legales y su control. El mismo reglamento (UE) 2016/679 trae consigo la posibilidad de que los países que hacen parte de esta directriz internacional puedan ampliar e incluso excluir de conformidad con los problemas internos, la normativa acogida, sin que esto represente un perjuicio a los principios que allí reposan (Redondo, 2020, p. 12).

En razón a lo anteriormente expuesto resulta importante traer a colación la ya nombrada Ley 3/2018, pues esta representa un refuerzo importante a la protección de los datos personales frente a los retos digitales que trae el nuevo siglo, la función de esta resulta ser pertinente de cara a los posibles aspectos que el legislador no haya tenido presente a la hora de expedir dicho reglamento.

Son 97 artículos los que conforman la Ley 3/2018, en ellos reposan garantías que entre otras cosas precisan, por un lado, la existencia de una serie de principios frente al control de los datos, así como la forma como estos serán manejados frente a su consentimiento. Abarcando también lo relacionado con los derechos de la seguridad digital en un aspecto amplio.

Por otro lado, también se precisa la protección de los menores en internet, fijando así una edad determinada en la cual el menor otorgue consentimiento frente al manejo de sus datos personales sin desconocer al titular de la patria potestad, pero si reconociendo el derecho constitucional que toda persona tiene. La normativa es tan nutrida que incluso menciona el procedimiento que debe seguirse en cuanto al tratamiento de los

datos cuando los menores y mayores de edad fallecen, otorgando así responsabilidad a sus representantes legales, cuando es el caso, con el fin de que no exista un desconocimiento de la información que quedó registrada (Redondo, 2020, p. 7).

Ahora bien, el artículo 70 de dicha Ley establece quienes deben cumplir con el tratamiento adecuado de los datos, es por ello que más adelante se mencionan las infracciones que pueden darse como resultado de un manejo irregular e inapropiado de los mismos, clasificándose estas en: *"muy grave, grave y leve*" (Ley 3 del 2018). Las primeras se dan como consecuencia de utilizar los datos con un fin distinto al solicitado inicialmente, por otro lado, el no informarle al titular de la información sobre el manejo de sus datos y adicional a ello cobrar una determinada suma de dinero para que puedan acceder a los mismos.

Las graves, por un lado, surgen frente a los datos de un menor y el mal manejo de estos, por ejemplo, el hecho de tener un control de su información personal sin contar con su previa autorización, por otro lado, este tipo de infracciones se configuran al no tener las medidas necesarias para garantizar la protección efectiva de los datos, y por último surgen de la evasión de no nombrar un encargado que salvaguarde los mismos (Redondo, 2020, p. 16).

Por último, las infracciones leves corresponden a todas aquellas en las que es quebrantado algún principio de transparencia, y en general incumplimientos normativos de carácter meramente formal establecidos en el artículo 74 de la Ley 3 del 2018.
Una de las novedades de la ley 3/2018 es la llamada "responsabilidad proactiva", la cual consiste en una serie de protocolos mediante los cuales se engloban principios relativos a la protección de los datos, esto por parte de un encargado designado por la respectiva entidad que retiene la información personal, con el fin de llevar un seguimiento donde el encargado sea capaz de demostrar que se cumple de manera eficaz los postulados de la ley (Garriga y Álvarez, 2020, pp. 13 -17).

Se evidencia entonces que España es un país cuya normativa se encuentra reforzada no solo por el reglamento general de protección de datos, si no por una normativa interna, reciente y amplia, que cubre grandes aspectos frente al manejo de la información personal, evitando así que surjan vacíos legales que atenten contra la seguridad jurídica.

Designed by Freepik

Conclusión

De conformidad con lo establecido en la diversa normativa que se presenta en el desarrollo del presente artículo, los datos personales resultan ser objeto de observación, análisis y tratamiento, ello en razón a la circulación masiva de la información, que a su vez surge como resultado de cambios socio culturales en los cuales se ha visto inmersa la implementación de nuevas tecnologías.

Motivo de lo anterior, el legislador procuró adoptar las medidas necesarias para garantizar la protección de datos, la

cual a su vez resulta relativa al ordenamiento del cual se esté precisando, en relación con el interés del presente artículo, Colombia cuenta con un sistema normativo, el cual en un inicio se centró únicamente a la relación de los datos con la vida crediticia (lo que no era suficiente para cubrir todos los aspectos que se reflejan en torno a la protección de datos).

Esto generó que Colombia se viera en la necesidad de extender su normativa, es por ello que surge la Ley 1581 de 2015, la cual cubre la protección de datos de manera general, tanto para entidades públicas como privadas, sin embargo, esta no se extendió lo suficiente para cubrir aspectos precisos, careciendo incluso de tratamientos exactos de cara a la responsabilidad del manejo de información.

Por otro lado, y contrastando el ordenamiento jurídico colombiano, se hace notorio que España cuenta con una regulación normativa que se desarrolló de manera más temprana, consiguiendo así en el trascurso del tiempo regulaciones más precisas, por lo que la circulación y tratamiento de datos se da bajo parámetros garantes de la salvaguarda de los derechos fundamentales que en la misma normativa se desarrolla.

Resulta entonces notorio el adelantado proceso en cuanto al tratamiento de datos que lleva España, pues como fue mencionado en el desarrollo del presente artículo, desde 1978 los legisladores se ocuparon de abarcar a grandes rasgos factores tales como el tecnológico, que resultaría un potente causante de diversas situaciones que iban a requerir atención normativa, es por ello que este país continuo evolucionando hasta el punto de tener precisión en asuntos tales como la protección de los datos y las garantías digitales.

Con base en esto España es un país que cuenta con una normativa que cubre aspectos que se adaptan a las necesidades que ha generado el nuevo siglo, por su parte Colombia hace su esfuerzo a fin de conseguir la protección integral de los datos, pero estos no han cubierto todos los aspectos necesarios para tal fin. Pese a los esfuerzos que ha realizado el legislador colombiano, se puede apreciar que algunos elementos de la normativa española e incluso de las directrices de la Unión Europea, podrían enriquecer la construcción de una normativa que garantice la mayor eficacia con relación al tratamiento de datos.

Referencias

Almagro. L, (2019). Clasificación de datos. *White paper series.* 6. 1-16. Recuperado de: https://www.oas.org/es/sms/cicte/docs/ESP-Clasificacion-de-Datos.pdf

Aguilar. M. (2018). La ley de protección de datos en Colombia: sus inicios y examen de sus principales postulados. (Trabajo de grado). Universidad Católica de Colombia. Bogotá, Colombia.

Botero. B y Martín. D. (2016). El valor de los datos personales en Colombia. *Revista CES Derecho*, 7 (1), 1-2. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2145-77192016000100001&lng=en&tlng=es.

Cristea. L. (2017). La ley de protección de datos en Colombia: sus inicios y examen de sus principales postulados. (Tesis Doctoral). Universidad Abat Oliba CEU.

Corte Constitucional, Sala plena. (16 de octubre de 2008). Sentencia C-1011-08. [MP. Jaime Córdoba Triviño].

Corte Constitucional, Sala plena. (06 de octubre de 2011). Sentencia C-748.11. [MP. Jorge Ignacio Pretelt Chaljub].

Días. C. (2017). ¿Tendremos nueva Ley de protección de datos en mayo de 2018? Recuperado de: https://cincodias.elpais.com/cincodias/2017/06/28/legal/1498636277_381690.html

Delegatura para la protección de datos personales. (2019). Guía para el tratamiento de datos personales para fines de marketimg y publicidad. *Superintendencia de Industria y Comercio.* https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20marketing%2C%20publicidad%20y%20tratamiento%20de%20datos%202019.pdf

Defensoría del pueblo. (s.f.). Políticas de protección de datos personales. *Transparencia y acceso a la información.* Recuperado de: https://www.defensoria.gov.co/public/ley1712/Protecciondedatosp ersonales.pdf

EquiSoft. (2017). La cadena de bloques (blockchain): Una tecnología disruptiva con el poder de revolucionar el sector financiero. Recuperado de: https://www.equisoft.com/wp-content/uploads/2017/09/White-paper-Blockchain-ESP-1.pdf

Fernández. P. (s.f.). Fundamentos de la protección de datos en España. *pablofb.com*. Recuperado de: https://www.pablofb.com/fundamentos-de-la-proteccion-de-datos-en-espana/

García. A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín mexicano de derecho comparado*, *40*(120), 743-778.

Gordillo. J y Restrepo. O. (2004). Introducción al análisis del derecho

fundamental del hábeas data. *Estudios Socio-Jurídicos*, *6*(2), 351-385.

Garriga. A y Álvarez. S. (2020) Aplicación del principio de responsabilidad proactiva al tratamiento de los datos personales en el ámbito del proyecto Securhome. Recuperado de: https://cenie.eu/es/blogs/securhome/aplicacion-del-principio-de-responsabilidad-proactiva- al-tratamiento-de-los-datos

Herrera. J, Agustinoy. A, Casas. R, Cerillo. A, Delgado. A, Jeffery. M, Morales. O, Oliver. R, Ormazábal. G, Vilasau. M y Xalabarder. R. (2004). Nociones técnicas de internet. Herrera. J. (Ed). *Derecho y nuevas tecnologías. (pp. 21-44).* Editorial UOC.

Suarez. F, Rodríguez. I, Bojórquez. J y Berdeja. M. (s.f.). Manual para la protección de datos personales. *Instituto Tabasqueño de Transparencia y Acceso a la información Pública, ittaip.org.mx*. Recuperado de: http://www.itaip.org.mx/reusdap/manuales/manual_datos_personales_ itaip.pdf

Jefatura del Estado. (18 de octubre de 2007). Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. [LO 25/2007]. BOE-A-2007-18243.

Jefatura de Estado. (07 de diciembre de 2018). Ley Orgánica de Protección de Datos Personales y garantías de derechos digitales. [LOPDPGDD 03/2018]. DO. BOE-A-2018-16673.

Liñayo. N. (2015). Definición de las Tecnologías de la Información y la Comunicación (TIC). *Universidad metropolitana de Caracas.* Recuperado de: https://sites.google.com/a/correo.unimet.edu.ve/2- equipo-4-eac-14152-fgtce04/home/definicion-de-las-tecnologias-de-la-informacion-y-la-comunicacion-tic

Martín, C. (2008). Legislación española sobre protección de datos y su implicación en la gestión bibliotecaria. Recuperado de: http://eprints.rclis.org/14305/1/prodatos.pdf

Muños, M. (s.f.). La protección de la persona frente a las tecnologías de la comunicación. *Archivos jurídicos unam.mx.* Recuperado de: https://archivos.juridicas.unam.mx/www/bjv/libros/5/2253/4.pdf

Maqueo. M, Moreno. J y Recio, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. Revista de derecho (Valdivia), 30(1), 77-96.

Rojas, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Universidad Católica de Colombia, NOVUM JUS.* 8(1). 107-139. ISSN: 1692-6013.

Redondo. B. (2020). El RGPD y la nueva LOPD: La protección de datos en España en 2020. Recuperado de: https://es.mailjet.com/blog/news/rgpd-lopd-proteccion-de-datos/

Recio. M. (2019). Protección de datos personales en la era digital: Evolución tecnológica. Conceptos básicos y elementos esenciales en materia de protección de datos. *Pontificia Universidad Javeriana.* Bogotá.

Recio. M. (2019). Protección de datos personales en la era digital: ¿Qué es la protección de datos personales? *Pontificia Universidad Javeriana.* Bogotá.

Recio. M. (2019). Protección de datos personales en la era digital: Nociones fundamentales sobre protección de datos personales. *Pontificia Universidad Javeriana.* Bogotá.

Superintendencia de industria y comercio. (2020). Sobre la protección de datos personales | superintendencia de Industria y Comercio. https://www.sic.gov.co/. https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Superintendencia de Industria y Comercio. (s.f.). Cartilla ley 1226 de 2008 habeas data. *Super Industria y Comercio.* Recuperado de: https://protecdatalatam.com/wp-content/uploads/2017/07/Cartilla_Ley_1266_de_2008_Habeas_Data.pdf

Tribunal Constitucional de España, Sala Primera. (20 de julio de 1993). Sentencia 4/1993. [MP. Francisco Javier Olaverri Zazpe].

Tribunal Constitucional de España, Sala Primera. (30 de noviembre de 2000). Sentencia 290/2000. [MP. Pedro Cruz Villalón].

Turbay. G. (2017). Atendiendo a la solicitud radicada ante esta Entidad a través su comunicación. *Superintendencia de Industria y Comercio*. Bogotá. Recuperado de: https://www.sic.gov.co/sites/default/files/files/Boletinjuridico/2017/RAD17005822ProteccionDatos.PDF

Turbay. G. (2018). Atendiendo a la solicitud radicada ante esta Entidad a través su comunicación. *Superintendencia de Industria y Comercio*. Bogotá. Recuperado de: https://www.sic.gov.co/sites/default/files/normatividad/022019/Rad18_18274412Datos.PDF

Ureña. A, Ferrari. A, Blanco. D y Valdecasa. E. (2012). Cloud Computing Retos y Oportunidades. *Observatorio nacional de las telecomunicaciones y de la SI.* Recuperado de: https://www.ontsi.red.es/sites/ontsi/files/1-_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf

Villabella, C. M. (2015). Los métodos de la investigación jurídica. Algunas precisiones. Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional. 2015. México. UNAM. 927