COOKIES PUBLICITARIAS, UN ARMA DE DOBLE FILO SIN PROTECCIÓN A LOS USUARIOS EN LA WEB

ANA MARÍA MESA GRANDA

Trabajo de grado para optar al título de abogado

Asesor

CARLOS ANDRES GOMEZ GARCIA

Abogado

UNIVERSIDAD PONTIFICIA BOLIVARIANA.

FACULTAD DE CIENCIAS POLÍTICAS-

DERECHO

MEDELLÍN

2022

9 de noviembre de 2022

Ana Maria Mesa Granda

"Declaro que este trabajo de grado no ha sido presentado con anterioridad para optar a un título, ya sea en igual forma o con variaciones, en ésta o en cualquiera otra universidad". Art. 92, parágrafo, Régimen Estudiantil de Formación Avanzada.

Firma del autor (es)

CONTENIDO

RESUMEN

La presente investigación tiene por finalidad analizar el tema referente a las cookies publicitarias y su regulación dentro del ordenamiento jurídico colombiano, definiendo las mismas como datos que le son extraídos a los usuarios que navegan en la web, lo anterior con el fin de crear una base de datos que pueda servir como herramienta de marketing, identificando y ayudando en temas publicitarios a empresas o diferentes fuentes para dar a conocer sus productos o servicios. El enfoque principal de este trabajo se desarrolla en torno a que estas entidades acceden a dicha información de forma imprudente, vulnerando la privacidad e integridad de estas personas al exponer datos valiosos e importantes albergados en la nube, provocando consecuencias negativas al desproteger por completo a los usuarios que desconociendo el funcionamiento y efectos que estas herramientas conllevan, pueden verse inmersos en problemáticas que afecten sus intereses.

El mundo por medio de las plataformas digitales y páginas web pueden conocer la vida de una persona con solo un clic. Países como Colombia al no establecer límites en su ordenamiento jurídico vigente, crea un mundo de posibilidades para todas estas compañías que quieran explotar todos estos datos, exponiendo así al usuario a múltiples peligros, desprotegiendo al mismo al existir una cantidad inimaginable de vacíos normativos con respecto a esta materia, mismos que ya han sido tratado por otras legislaciones que pueden servir como base para la construcción de una legislación renovada que responda a las necesidades que plantea el panorama actual en lo referente a la protección de datos.

Palabras Claves: cookies publicitarias, privacidad, base de datos, web, protección, legislación, usuario, nube.

ABSTRACT

The purpose of this research is to analyze the issue regarding advertising cookies and their regulation within the Colombian legal system, defining them as data that are extracted from users who browse the web, the above in order to create a database of data that can serve as a marketing tool, identifying and helping companies or different sources with advertising issues to publicize their products or services. The main focus of this work is

developed around the fact that these entities access said information recklessly, violating the privacy and integrity of these people by exposing valuable and important data stored in the cloud, causing negative consequences by completely unprotecting the users. users who, unaware of the operation and effects that these tools entail, may find themselves immersed in problems that affect their interests.

The world through digital platforms and web pages can learn about a person's life with just one click. Countries like Colombia, by not establishing limits in their current legal system, create a world of possibilities for all these companies that want to exploit all this data, thus exposing the user to multiple dangers, leaving them unprotected as there are an unimaginable amount of regulatory gaps regarding to this matter, same that have already been treated by other legislations that can serve as a basis for the construction of a renewed legislation that responds to the needs posed by the current panorama in relation to data protection.

INTRODUCCIÓN

Las cookies publicitarias se pueden definir como aquellos datos que extraen diferentes empresas y compañías con el fin de hacer publicidad, llegando así de manera más eficiente a su público final. De esta manera usan la información privada de los usuarios para satisfacer sus necesidades, sin tener límites, a causa de la ausencia de regulaciones jurídicas sólidas, que establezcan mecanismos o procedimientos que faciliten la protección de la información de estas personas. La actividad que realizan los captadores de esta información es temeraria en el sentido que exponen dicha información de la forma que podría afectar la privacidad y seguridad de los usuarios. Aunque si bien, dicha información en principio puede ser extraída con fines positivos, pues se debe reconocer que las cookies han servido como herramienta fundamentales para que miles de empresas distribuidoras de bienes y servicios localizadas en la web, pudieran encontrar posibles interesados en sus productos y aumentar de dicha forma el número de clientes, pero, el problema surge al analizar que filtros utilizan estas para que la información utilizada no recaiga en personas que busquen darle un mal uso a la misma, siendo incontables los casos en los que la seguridad de miles de usuarios ha sido vulnerada a raíz del acceso de personas mal intencionadas a bases de datos con información de tipo privado.

Para analizar esta problemática es necesario mencionar sus causas, destacando dentro de las mismas la falta de regulación y eficiencia de las normas que regulan esta materia. Se entiende esto como las vulneraciones que pueden cometer con esta información al carecer de límites claros, que ayuden a la protección de las personas que navegan en la web. Los que usan están cookies publicitarias son personas que el único fin que buscan es un provecho económico y comercial a costa de la información suministrada por los usuarios, actividad que se ha visto en aumento ante la ausencia de una norma clara y expresa que realmente cubra las necesidades actuales en cuanto a seguridad informática se refiere, quedando la mayoría de estos en la pura impunidad y sin casi que más remedio para las víctimas de estos sucesos que olvidar lo acontecido y confiar casi que ciegamente en que sus datos no sean vulnerados en futuras ocasiones.

CAPÍTULO 1

La evolución jurisprudencial en Colombia en materia de protección de datos y cookies publicitarias.

¿Qué son las cookies publicitarias y cuál es su impacto en la protección de datos almacenados en la web?

Las cookies publicitarias han aparecido en el mundo del internet como una herramienta novedosa e incluso desconocida para muchos de los internautas, pero, de gran auge durante los últimos años ante la cada vez mayor necesidad de dar un paso hacia la digitalización, en mayor medida, por parte de personas que han decidido trasladar o crear sus negocios dentro del mundo web. Este instrumento, ha servido como un método de monitorización que ha permitido a miles de nuevos emprendedores encontrar potenciales clientes a través del rastreo de datos inteligente, es decir, llegando a los mismos a través de la búsquedas que los mismos usuarios realizan en internet, los sitios web que visitan, la información compartida en redes sociales, datos que no solo permiten identificar los gustos generales de la comunidad en temas de oferta y demanda, sino también, acceder a datos personales como lo puede ser el nombre, apellidos, correo electrónico, número de contacto o dirección, los cuales si bien pueden ser de gran utilidad en las manos de quien realmente desee utilizar dicha herramienta con fines publicitarios, pero a su vez, exponiendo dicha información ante posibles riesgos debido al fácil acceso que las cookies permiten sobre los mismos.

Pero, para poder desarrollar de forma completa el tema de las cookies, es necesario saber en qué consisten las mismas. El autor Lope Jiménez David se refiere al tema diciendo que

> Las cookies son pequeños ficheros de texto, a menudo encriptados, que contienen información y se almacenan en el navegador o en el disco duro de tu ordenador. Estos ficheros de datos se crean al cargar una página web concreta. El servidor de la página web envía la información a nuestro navegador, creando este un archivo de texto. Cada vez que el usuario vuelve al sitio web, la página web recupera el archivo de texto a través del navegador, permitiendo al servidor de la página recuperar toda la información previamente registrada. (Lopez Jiménez, David. (Lopez, 2011)

Lo anterior, permite identificar el alcance de almacenamiento en cuanto a la cantidad de datos que dicha herramienta puede llegar a almacenar, teniendo dicha recolección como finalidad principal, primero, la de recordar si el usuario ha interactuado o no anteriormente con un tipo de página web, con el fin recomendar o no a este algunas del mismo tipo o facilitar su acceso a través del almacenamiento de información como correos o contraseñas o, segundo, conocer los intereses del usuario con el fin de ofrecer al mismo productos o servicios relacionados con la información almacenada, esto, siempre y cuando la cookie sea usada con la motivación real que se busca alcanzar con la misma, ya que, es necesario advertir que además de los usos anteriormente mencionados, se han podido detectar como, a través del uso de las mismas, usuarios mal intencionados han accedido a este tipo de información con objetivos fraudulentos. Aunque si bien, se han tomado medidas casi que a nivel global para regular este tipo de herramientas, tales como lo son, la obligatoriedad en cuanto a los sitios web de avisar al usuario acerca del uso de cookies, el requerimiento de que el usuario acepta el uso de la cookie, entre otros, en muchos casos estas se han quedado cortas pues no alcanzan a reflejar el peligro al cual el usuario se somete.

Pero, el verdadero problema surge cuando estas cookies, además de exponer el historial e información del usuario, también deja al aire datos personales, de contacto o información crediticia del usuario, pues la misma expone en gran manera derechos fundamentales como lo son la libertad y la privacidad. Como datos personales debemos entender, según el concepto dado por el autor Jorge Vergara

> Un dato personal es cualquier información relativa a una persona física viva identificada o identificable. Entendiendo que la persona está identificada cuando el dato hace referencia a una persona concreta cuya identidad se conoce. Por el contrario, la persona será identificable cuando se desconoce su identidad, pero se podría llegar a averiguar. (…) El dato puede ser una información gráfica, fotográfica, acústica, alfabética, numérica o de cualquier otro tipo. Lo importante para que sea considerado personal es que con él se identifique o se pueda llegar a identificar a la persona a la que hace referencia esa información. (Vergara, 2019)

Los datos personales de una persona hacen parte de su núcleo más íntimo, pues permiten individualizar a una persona haciéndola identificable, lo cual, no es un problema mientras esta información se mantenga reducida al círculo de confianza de un individuo, pero, cabe mencionar que, a través de la aparición de las redes sociales y la navegación web, ese círculo se ha hecho mucho más grande, siendo cada vez mayor el hecho de que dichos datos sean compartidos no solo por los mismos usuarios en sus interacciones virtuales, sino también, por el irresponsable uso que muchas entidades le dan a los mismos, compartiendo estos sin discriminación alguna o en algunos casos, almacenando dicha información sin ningún tipo de seguridad o filtro que evite el ingreso de tercero a dicha información que el usuario brinda a ciertos sitios que considera de confianza.

La intimidad, como derecho, representa "la facultad destinada a salvaguardar un determinado espacio con carácter exclusivo, y que consistía en un derecho del individuo a la soledad y a tener una esfera reservada en el cual desenvolver su vida sin que la indiscreción ajena tenga acceso a ella" (Gonzales, 2007).

Como todo derecho, la intimidad no es absoluta, abarca ciertos temas que puedan afectar la vida personal, familiar o social del individuo, un aparte que se encuentra restringido siempre y cuando dicha intimidad no afecte o ponga el riesgo el derecho de un tercero. Aunque es lógico pensar que, ese límite es cada vez más delgado con los avances tecnológicos en el campo de la comunicación y dicha información, a través de herramientas

como las cookies, es de conocimiento cada vez más de un número mayor de personas, sin ser esto legalmente una intromisión a ese derecho, sin embargo, el detonante se encuentra en el uso que se le pueda dar a esa información y cómo afecta ese uso la seguridad y libertad del usuario. Dicho derecho se encuentra consagrado en el artículo 15 de la constitución política de Colombia, el cual dicta que "ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.", estableciendo no solo dicho derecho sino además la obligación del Estado de proteger y garantizar el mismo.

Todo lo anterior, hace de las cookies una figura bastante amplia, siendo un instrumento de gran ayuda para una época en la cual se ha hecho cada vez más urgente el uso de las redes por parte del comercio, donde la necesidad de emprender ha llevado a que las personas busquen llegar al máximo número de usuarios posibles para ofrecerles objetos de su posible interés de una manera fácil y sencilla, ejerciendo casi que una comunicación directa con los mismos, pero que también, debe analizarse desde el punto de vista de los peligros que existen en internet, de la existencia de personas que se aprovechan de este tipo de medios con fines ilícitos y la posición de desprotección en la cual colocan a los usuarios incluso en muchos casos, sin el conocimiento de los mismos acerca de dichos peligros.

1.2 Evolución de las cookies publicitarias

Aunque se considere una figura novedosa, las cookies aparecieron durante el año de 1994, siendo su creador un trabajador de NETSCAPE, el cual se encargó de almacenar la información de los distintos usuarios que ingresaban a la web de su empresa, guardando los artículos favoritos de los mismos dentro del carrito de compras de la página, de forma que se consumieran menos recursos de la página y se agiliza la gestión de esta. El problema que surgió en torno a esta primera aparición es que se hizo sin el permiso o autorización de los usuarios, lo cual, posteriormente, generaría bastante conflictos, siendo esto retratado por un artículo de The Financial Times, describiendo los distintos casos que habían llegado hasta la

Comisión Federal de Comercio lo cual hizo que el tema se sometiera a distintos estudios, en este se determinó que esta herramienta constituía un verdadero peligro para la seguridad de los datos de los usuarios almacenados en la web y al ser cada vez mayor el número de empresas que incorporan las mismas sin dar aviso a sus clientes, lo cual llevó a que distintas legislaciones determinan que era obligatorio dar aviso a los mismos acerca de la existencia de cookies dentro de sus páginas y a que su vez los usuarios pudieran aceptar o no el uso de las mismas en su navegación.

Ante los nuevos desafíos que poco a poco iba planteando la cada vez más extensa web, se fue haciendo mayormente necesario un sistema de protección, de normas o un mayor número de restricciones que impidieron la recolección de datos sin autorización de los usuarios en línea, además, también era necesario comenzar a proteger la información de terceros malintencionados que pudieran acceder a la misma, ya que además de contar con el consentimiento de sus usuarios para poder llevar a cabo esta recopilación de datos, también debían asegurar que los mismos no serían usados para finalidades distintas a las informadas, de no transmitir esa información a otras entidades o usuarios y además, adquirían el deber de proteger esos datos mientras estuvieran en su poder.

En cuanto a Colombia se refiere, a pesar de que durante la última década se ha empezado a darle una mayor relevancia al tema, poca es la jurisprudencia en materia de protección de datos, pudiendo encontrar sólo algunos aportes sobre el tema, tal como el concepto de la Superintendencia de Industria y Comercio, la cual, a través de su página web, realizó una observación a modo explicativo del tema diciendo que

> Las cookies son archivos que recogen información a través de una página web sobre los hábitos de navegación de un usuario o de su equipo y eventualmente podrían conformar una base de datos de acuerdo a la definición legal de la Ley 1581 de 2012 al recolectar datos personales conforme a las siguientes características: (i) están referidos a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el

> titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación; caso en el cual, el responsable deberá ceñirse por las normas sobre protección de datos vigentes en Colombia, en especial la aplicación de los principios rectores para la administración de datos de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad consagrados en el artículo 4 de la Ley 1581 de 2012. (SIC, 2016).

Además de la Superintendencia de Industria y Comercio, el Congreso de la Republica ha dado su granito de arena a través de la Ley 1273 de 2009 "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"(…)" y de la ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales.", normas las cuales ayudaron a nutrir la poca regulación existente a nivel nacional acerca de la protección de datos, que aunque no se refieren directamente al temas de las cookies publicitarias, si suben un escalón el nivel de protección de los datos de los usuarios en la web, estableciendo por primera vez sanciones y garantías reales a los derechos de los internautas.

1.3 Normativa vigente en Colombia

Actualmente, Colombia cuenta con una legislación bastante limitada en el tema de protección de datos, pudiéndose destacar principalmente dos leyes vigentes, las ya mencionadas Ley 1273 de 2009 y Ley 1581 de 2012, las cuales se refieren a los delitos información, seguridad en línea y protección de datos en la web.

La ley 1273 de 2009, la cual se encarga de introducir al sistema jurídico colombiano las primeras normas al código penal acerca de delitos informáticos, clasificándolos en atentados contra la confidencialidad y delitos contra la integridad y la disponibilidad de los datos y de los sistemas informáticos; de los atentados informáticos y otras infracciones. Estos delitos fueron añadidos al Código Penal bajo el título de la Protección de la información y de los datos

Por su parte, la ley 1581 de 2012 se refiere al tema de la protección de datos principalmente, estableciendo su objeto en el artículo primero de la misma ley diciendo que

> "***Objeto*.** La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma." (Ley 1581, 2012)

Establece que, en principio, la regulación se aplicará a aquellos datos personales registrados en bases de datos que sean susceptibles de ser usados por entidades públicas o privadas ya sea en territorio colombiano o que quien esté a cargo de los mismos, bajo las reglas del derecho internacional, se someta a la ley colombiana. El artículo dos menciona que dicha ley no se aplicara a las bases de datos o archivos del ámbito personal o domestico; a las bases de datos o archivos sobre seguridad y defensa nacional, sobre la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo; a las bases de datos de información periodística y contenidos editoriales; a las bases de datos reguladas por la ley 1266 de 2008 y a las bases de datos reguladas por la ley 79 de 1993. Además, establece también los principios para el tratamiento de datos personales los cuales son el principio de legalidad en materia de tratamiento de datos, principio de finalidad, principio de libertad, principio de veracidad o calidad, principio de transparencia, principio de acceso y circulación restringida, principio de seguridad y el principio de confidencialidad. Actualmente, esta ley representa el mayor referente dentro de la legislación nacional en cuanto a normas de protección de datos se refiere.

Posteriormente a la expedición de la ley 1581 de 2012, se expide el decreto 1377 de 2013, el cual, ampliando el margen de protección que ya venía trabajándose con la ley antes mencionada, trabaja el tema del Habeas Data, tema que al igual que el anterior, tiene una gran conexión con el tema relacionado al uso de cookies publicitarias y es lo concerniente a la autorización que debe dar el usuario para que sus datos personales sean utilizados, también

trata el tema concerniente a las políticas de tratamiento de los responsables y encargados, la transferencia de esos datos personales del usuario, los derechos en cabeza del titular de la información y la responsabilidad que cargan las entidades que manejan dicha información. El artículo quinto y sexto de la ley mencionada, habla acerca del tema de la autorización del uso de datos personales e íntimos diciendo que

> Artículo 5°. Autorización. El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento. (…) Artículo 6°. De la autorización para el Tratamiento de datos personales sensibles. El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley. (Ley 1377, 2013).

En la legislación colombiana no se estipulan normativas concretas, creadas con el fin de regular este tema en específico. Muchas empresas y usuarios usan estos datos sin limitaciones propiamente aplicadas al tema, lo que genera un amplio margen de posibilidades respecto a la información que estos extraen. Si bien la normatividad está relacionada con procedimientos para solicitar los datos de los usuarios en la web, no existen disposiciones claras acerca del uso posterior de estos, dejando en gran desprotección los derechos de los usuarios anteriormente mencionados.

CAPÍTULO 2

Protección de datos y cookies publicitarias en el derecho comparado e internacional

Cómo ya se ha dicho anteriormente, actualmente Colombia ha tenido un pobre desarrollo legislativo en cuanto a la regulación de la protección de datos de los usuarios que navegan en la web, esto a pesar del estallido que han traído consigo las redes sociales, el cada vez más común uso de sitios web para facilitar la comunicación entre pequeñas y grandes empresas con sus clientes y el cada vez en aumento mayor número de personas que usan el internet para cualquier actividad posible dentro de su vida diaria, lo cual es una muestra de que la necesidad de una regulación expresa, vigente y actualizada habrá lugar dentro del ordenamiento debido a que, ante el mayor uso de las redes, mayor es el número de posibles víctimas que se exponen a qué sus datos sean usados de forma malintencionada por cualquier otro usuario en línea. Pero, el hecho de que la legislación colombiana se haya quedado atrás, no quiere decir que en otros ordenamientos jurídicos distintos efectivamente si exista una regulación que, contrario al caso colombiano, entregué a los usuarios herramientas jurídicas que permitan brindarles una mayor seguridad mientras éstos navegan por los distintos medios que internet brinda a sus usuarios, ya que, permiten establecer mecanismos de seguridad previos o, en caso de haber ocurrido ya la infiltración en los datos personales de alguno de los individuos, le presenta al mismo la posibilidad de tomar acciones no solo contra aquel que haya cometido dicha actividad ilegal sino también contra aquella entidad o individuo que debía velar por la protección de dichos datos.

Acerca del tema, el autor Itziar Damborenea Trigueros, argumenta que, dentro del sistema de derecho internacional, existen a nivel internacional 107 países que actualmente posee una normativa vigente acerca de la protección de datos, extrayendo dicha información del estudio realizado por la Conferencia de las Naciones Unidas sobre el Comercio y Desarrollo (UNCTAD), citando el autor entre muchos

> PIPEDA (2000) en Canadá, el Privacy Act (1988) en Australia, el Federal Law Regarding Personal Data (2006) en Rusia, la Ley Orgánica de Protección de Datos

> Personales y la garantía de los derechos digitales (o «LOPDGDD») (2018) en España o la Ley de Protección de Datos Personales (2000) en Argentina. A nivel supraestatal, encontramos el RGPD (2016) en Europa, el Framework on Personal Data Protection (2016) de ASEAN o la Convención en ciberseguridad y la protección de datos personales (2019) de la Unión Africana (o «UA»). (Trigueros, 2020)

Lo anterior, permite identificar que a nivel internacional existen un gran número de países que, a diferencia de Colombia, se han puesto manos a la obra con el problema que representa la protección de los datos de los usuarios en línea, destacando el autor citado que, entre estás regulaciones, existen lógicamente diferencias que se caracterizan principalmente por el número mayor o menor de restricciones que existen por parte de las entidades a la hora de manejar estos tipos de datos en sus bases datos, destacando entre los mismos el sistema utilizado por la Unión Europea, la cual, se encargó de unificar las distintas legislaciones en dicha materia para crear un único Reglamento General de Protección de Datos, el cual ha sido reconocido en la materia como el más estricto a nivel global, pues impone una serie de obligaciones que representan una carga de responsabilidad bastante grande para las entidades que en sus bases de datos alberguen datos personales de sus usuarios, ya que, reconoce la importancia de esos datos y por tanto impone a la las entidades un deber de protección de los mismos, todo esto siendo un punto a favor de la comunidad pues se incentiva a los sitios web a hacer un uso precavido y correcto de sus distintas plataformas, además desincentiva cualquier actuación contraria a la ley a través de la imposición de altas y cuantiosas sumas que servirán como retribución a aquella persona que se vea afectada por este tipo de actos, las cuales pueden rondar “hasta los 20 millones de euros como máximo o tratándose de una empresa de una cuantía equivalente al 4% como máximo del volumen del negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía” (Trigueros 2020), las cuales no solo estarán a cargo del individuo o individuos que lleven a cabo la violación a la privacidad de los mismos sino también a la entidad que los tenía en su poder y que fallo a la carga impuesta por las normas vigentes.

El mismo autor además, resalta que al igual que existen diferencias que permiten caracterizar los distintos ordenamientos en relación a sus políticas y leyes acerca del tratamiento de datos,

también existen ciertos aspectos similares y que se repiten en general en estos 107 países. Principalmente, son tres las características que suelen repetirse dentro de estas regulaciones, la primera, siendo la aplicación de los principios generales, comunes en casi todos los ordenamientos jurídicos y por tanto, encontrándose estos como una base importante en cuanto a la construcción de una normativa de un problema que afecta a casi todos los países a nivel mundial. En segundo lugar, se debe decir que en la mayoría de estos países, se han creado entidades encargadas de cumplir con tareas de supervisión y control que permiten velar por el correcto cumplimiento de estos sistemas normativos, siendo este punto profundizado por el mismo Trigueros acerca del cual se expresa diciendo que

> La mayoría de Estados que han adoptado una regulación en materia de protección de datos o privacidad han establecido agencias estatales encargadas de supervisar el cumplimiento de la misma. Por ejemplo, en España nos encontramos con la Agencia Española de Protección de Datos, en Inglaterra con la Information Commisioner's Office, la Office of Privacy Comissioner en Canadá o Roscomnadzor en Rusia. En el otro lado de la balanza se encuentra EEUU, país donde no existe una APD central sino distintas agencias sectoriales o estatales. La mayoría de APD funcionan como órganos consultivos y de control que poseen poderes sancionadores y ante los cuales pueden ejercerse derechos y presentarse reclamaciones. La autoridad y competencias de las mismas dependerá de cada régimen jurídico. (Trigueros, 2020)

Cómo último punto similar entre los distintos ordenamientos jurídicos que se han pronunciado legislativamente sobre la materia, se encuentra el punto consistente en qué los mismos cuentan con un sistema que tiene por finalidad limitar el traspaso de datos entre terceros países, regulación que claramente favorece la protección de los datos privados de los distintos usuarios en la web pues se reconoce el peligro que puede correr dicha información en un posible traslado de tan gran magnitud, por lo cual, el sistema jurídico se encarga de imponer cargas más gravosas para aquellos casos en los cuales dicho intercambio sea necesario o se planee llevar a cabo, ya que es una actividad que arriesga la intimidad de los usuarios en favor de terceros.

Ya habiendo tocado el tema de las similitudes y diferencias existentes entre un sistema y otro

a la hora de tratar el tema de la protección de daría, es importante advertir que a través de la historia han existido además intentos por generar un sistema global unificado, ya que, cómo se expuso con anterioridad, el tratamiento de datos personales de los usuarios que navegan en la web ha sido un problema de índole global, viendo este sus consecuencias alrededor del mundo sin importar la rigurosidad que los mismos Estados manejen a la hora de tratar dicho tema. Iniciativas cómo el Fair Information Principles propuesto por los Estados Unidos en 1973, el sistema propuesto por la Organización para la Cooperación y el Desarrollo Económico (OECD) o la Convención para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en la Unión Europea, siendo este uno de los más importantes en la materia, pues aún se encuentra vigente y ha abierto su campo de aplicación a cualquier otro país por fuera de la Unión Europea que quiera ratificar el mismo. Todos los anteriores han sido intentos de unificar la regulación existente, lo cual, aunque en sí, no plantea una solución a todos los problemas que puedan enfrentar los usuarios en la web, si permitiría unificar las soluciones existentes y conocidas a día de hoy contra este tipo de problemas.

Por otra parte, retomando la regulación vigente que la Unión Europea maneja en materia de protección de datos, debe destacarse que la misma fue sometido a un proceso riguroso introduciendo las novedades que se querían implementar de forma progresiva, permitiendo identificar el impacto que las mismas normas tendrían en la utilización de los datos e información privada de los usuarios en la red. Acerca del tema, la autora Sofía Ruiz de la Viuda, se pronunció acerca del tema hablando de la evolución que ha tenido el sistema vigente de protección de datos a partir de la introducción del Reglamento 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, acerca de lo cual se expresó diciendo que

> Las tecnologías digitales de la información han sufrido, desde la publicación del texto que este Reglamento deroga, cambios fundamentales y solo han crecido en importancia y en implantación social, por lo tanto, antes de la publicación en 2016 de este Reglamento, las autoridades europeas también llevaron a cabo, a través de decisiones, comunicaciones y sentencias del Tribunal de Justicia de la Unión, ciertos

> cambios en la aplicación de la Directiva 95/46, en pos de garantizar una mayor seguridad a sus ciudadanos (de la Viuda, 2019).

Dicha regulación, a traído consigo una gran cantidad de novedades que van servido como fundamento para la protección de este información privada en internet, esto es, el derecho que tienen los individuos a exigir a los distintos dueños de servidores o bases de datos en línea que, cuando lo soliciten, eliminen sus datos una vez estos no quieran que los mismos se encuentren dentro de estos sistemas, lo cual representa una nueva ventaja en favor de los usuarios, ya que el uso de sus datos se verá limitado en la medida que estos mismos deseen que se encuentren almacenados en los distintos sitios web, cosa que, aunque en principio podría parecer lógica, permite ahora que los distintos usuarios tengan una herramienta legal para reclamar el cese del uso de su información privada por aquellas entidades a las cuales estos mismos quieran limitar el acceso. El autor, Antonio Troncoso Reigada, a través de su texto habla acerca del tema destacando el papel fundamental que ha traído consigo la evolución del sistema normativo europeo en materia de protección de datos, siendo el derecho de rectificación y de supresión o cancelación de datos uno de los grandes avances del mismo, acerca de lo cual dice que

> De esta forma, se reconoce expresamente el derecho de los usuarios a exigir a los proveedores de estos servicios de Internet que borren completamente sus datos personales –por ejemplo, sus fotos– cuando el cliente se dé de baja en el servicio o cuando dejen de ser necesarios para los fines para los que se recabaron. Además, se establece expresamente que cuando "el responsable haya hecho públicos los datos personales, éste está obligado a adoptar las medidas razonables –incluidas las técnicas– en lo que respecta a los datos de cuya publicación sea responsable con miras a informar a los terceros que están tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a estos datos personales, o cualquier copia o réplica de los mismos (Reigada, 2012)

Pero, el sistema implementado no solo se limita a la responsabilidad que tienen la entidad que tiene dichos datos en su poder y en el uso de los mismos, sino también, en el uso que terceros hayan podido darle a esa información suministrada por el principal responsable, es

decir, aquella entidad que de manera inicial tenía acceso a la información, diciendo que, dicha entidad principal tiene por objeto no solo cesar el uso de la información privada del usuario que así lo solicite, sino que, además, tiene la obligación de dar dicha información a terceros, siendo en la mayoría de casos los buscadores como Google o Yahoo, los cuales replican en muchos casos la información suministrada a través de publicaciones. Acerca de este problema, Troncoso explica que

> La regulación del derecho al olvido que hace la propuesta de Reglamento establece una obligación del responsable de la publicación de los datos en Internet, no solo de suprimir los datos personales sino de comunicar a terceros que están tratando dichos datos que el interesado solicita que se suprima cualquier enlace, copia o réplica de los mismos, relacionando una cosa con la otra, y exigiendo al responsable de la primera publicación que adopte "todas las medidas razonables, incluidas las técnicas", lo que, a nuestro juicio, le obliga a implantar mecanismos que impidan la indexación –aunque esta obligación de implementar tecnología que impida la difusión generalizada debería aparecer con más claridad en la propuesta de Reglamento–. (Reigada, 2012).

En conclusión, otros países podrían servir como un referente al momento de reformar y agregar contenido a la normativa colombiana. Estos elementos son de gran utilidad, de tal manera que puedan haber mayores herramientas al momento de proteger a los usuarios que proporcionan sus datos. Debemos implementar estas disposiciones con el fin de realizar una comparación y ponderación de las disposiciones que faciliten el entendimiento de las leyes colombianas, y, además sirven para imponer límites a aquellos que quieran dar un mal uso a esta información.

CAPÍTULO 3

Impacto jurídico de la aparición de las cookies publicitarias y el peligro que representan a la seguridad de los datos.

Como se ha mencionado anteriormente, internet se ha convertido en un lugar bastante concurrido con un número casi que incontable de usuarios alrededor del mundo, del cual, un gran porcentaje utiliza las redes y los distintos sitios web con fines totalmente lícitos como lo pueden ser su uso con fines comunicativos, para conocer nuevas personas alrededor del mundo, investigar información de manera más fácil, realizar transacciones en línea o publicitar sus negocios en internet para llegar al mayor número de clientes posibles. Pero, así como existe un gran número de personas que utilizan estos medios para los fines a los cuales realmente sirve, también dentro de la comunidad en línea existen distintas personas que, se han servido de este tipo de herramientas para llevar a cabo fines ilícitos, como lo pueden ser el uso de hardware malicioso para tener acceso a los datos personales de los usuarios, para robar información bancaria o incluso realizar transacciones ilegales por medio de internet.

En cuanto a las cookies publicitarias se refiere, en un principio, las mismas se crearon con el fin de facilitar a distintos sitios, la recolección de datos de los distintos usuarios que navegan por la web, creando bancos de datos que les permitiera crear una base de información referente a las posibles personas a las cuales quisieran llegar, siendo mas usado por empresas que encuentran su domicilio en internet, permitiendo facilitar la promoción de sus productos o servicios, pero, a si como se ha usado el internet para realizar actos que se pueden considerar como ilícitos, también han aparecido en diferentes ocasiones casos en los cuales los dueños de estos sitios utilizan las cookies con el fin de recolectar información para transmitir la misma a terceros sin la aprobación del usuario, lo cual puede ser considerado una violación a la privacidad del individuo o también, se han podido percibir que en muchos de estos actos puede no existir dolo o culpa sobre la cabeza de la persona que administra el sitio web, sino que, al carácter de un sistema de seguridad sobre estas bases de datos, suele ocurrir que la información sea filtrada por terceros que aprovechan sus habilidades para acceder a este tipo de bases privadas.

En el ordenamiento jurídico internacional, este tipo de actos se encuentran regulados de una forma más precisa, pues se debe decir que aunque a nivel nacional Colombia cuenta con su propia regulación acerca de la protección de datos, esta no se encuentra tan desarrollada a comparación de otros ordenamientos jurídicos, en los cuales, a través de la experiencia, la

investigación y el desarrollo jurisprudencial de las mismas, han logrado regular un mayor número de supuestos en los cuales la seguridad de los usuarios en línea se pueda ver violada por otros usuarios malintencionados que traten de darle un uso incorrecto o prohibido a los datos personales almacenados en sitios web acerca de los distintos usuarios que tienen un perfil en línea.

En desarrollo de lo anterior, en materia de vigilancia, la ley colombiana contempla a través de la Ley 1266 de 2008, que será la Superintendencia de Industria y Comercio quien se encargará de que se cumplan los deberes impuestos a las distintas entidades que, en el ejercicio de sus actividades, manejen, compartan o distribuyan información de sus usuarios, y que, en los casos de que alguna de esas entidades sea supervisado por la Superintendencia financiera, será esta última la encargada de vigilar y castigar a las mismas en lo relativo al manejo de información.

> La Superintendencia de Industria y Comercio ejercerá la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, en cuanto se refiere a la actividad de administración de datos personales que se regula en la presente ley.
>
> En los casos en que la fuente, usuario u operador de información sea una entidad vigilada por la Superintendencia Financiera de Colombia, esta ejercerá la vigilancia e impondrá las sanciones correspondientes, de conformidad con las facultades que le son propias, según lo establecido en el Estatuto Orgánico del Sistema Financiero y las demás normas pertinentes y las establecidas en la presente ley. (Ley 1266, 2008)

En contraposición a lo anterior, en el derecho internacional, más precisamente en la regulación europeo unificada, citando nuevamente al autor Reigada, este establece que el usuario tiene derecho a reclamar acerca del uso que le dan las distintas entidades a la información que el mismo brinde, derecho que incluso le da la posibilidad de solicitar a la entidad que el uso de esta información sea pausado, viéndose en la obligación la entidad de borrar y dejar de utilizar cualquier registro sobre los datos personales almacenados en sus bases de datos sobre el usuario en cuestión, obligación que, se extiende a terceros en los casos

en que estas entidades hayan compartido por algún motivo u otro la información, recayendo sobre esta la responsabilidad acerca de que dichos terceros cumplan o no con esta orden de suprimir el contenido. Esto es, se establece una regulación pro garantista de los derechos fundamentales del usuario, siendo mas precisos, al derecho fundamental reconocido como Habeas data, incluso protegiendo al usuario cuando sus derechos choquen con la actividad común de la entidad sobre la cual se dirija.

> De esta forma, se reconoce expresamente el derecho de los usuarios a exigir a los proveedores de estos servicios de Internet que borren completamente sus datos personales –por ejemplo, sus fotos– cuando el cliente se dé de baja en el servicio o cuando dejen de ser necesarios para los fines para los que se recabaron. Además, se establece expresamente que cuando "el responsable haya hecho públicos los datos personales, éste está obligado a adoptar las medidas razonables –incluidas las técnicas– en lo que respecta a los datos de cuya publicación sea responsable con miras a informar a los terceros que están tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a estos datos personales, o cualquier copia o réplica de los mismos (Reigada, 2012)

Ahora, hablando de las sanciones en el ordenamiento jurídico colombiano, podemos encontrar su regulación en la ley estatutaria 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales" (Ley 1581 de 2012), en su titulo séptimo, capitulo primero, establece las sanciones aplicables por parte de las autoridades encargadas de la vigilancia, control y con la potestad sancionatoria sobre aquellas empresas o entidades que entre sus actividades manejen bases de datos que contengan información personal de sus usuarios. La ley acerca del tema establece que

> La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:
>
> a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que

las originó;

b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;

c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;

d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles. (Ley 1581 de 2012)

Además, la ley también se encarga de determinar los criterios a tener en cuenta al momento de graduar la sanción, tarea que, cumple en su artículo 24, a través del cual dice que se tendrá en cuenta la dimensión del daño o peligro que se cause; el beneficio económico que obtenga el infractor; la reincidencia; la resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia; la renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio y el reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar. Además, es importante destacar que esas sanciones consagradas en los artículos 23 y 24 de la Ley 1581 de 2012, según el parágrafo del articulo 23, solo son aplicables a entidades de derecho privado, tratándose de entidades reguladas por la Superintendencia de Industria y comercio, ya que, en los casos en los cuales se trate de una violación por parte de la entidad pública, esta deberá remitir la información a la Procuraduría General de la Nación para que adelante la respectiva investigación.

CONCLUSIONES

En conclusión, aunque si bien, la legislación colombiana ha abordado el tema de la protección de datos personales en internet, los cuales indirectamente, regulan algunos aspectos importantes en cuanto al uso de cookies se refiere, es necesario recalcar que dicha normativa está llena de lagunas y vacíos que siguen dejando ciertos puntos vulnerables en cuanto a la

recolección de información personal e íntima por parte de las distintas bases de datos programadas a través de las distintas páginas web que se pueden encontrar en la red y que, por lo mismo, es necesario buscar, ya sea en la jurisprudencia, doctrina o en otras jurisdicciones, soluciones que permitan complementar la regulación colombiana en materia de protección de datos, más específicamente, en cuanto al uso de cookies publicitarias se refiere.

el sistema jurídico internacional trae consigo una gran novedad de sistemas normativos aplicables a la materia de protección de datos e información de tipo personal suministrada por los usuarios en la web, encontrando que entre los distintos países que tienen una legislación vigente, existen distintos tratamientos a la materia, algunos más estrictos y con una imposición mayor de cargas a las entidades que se dedican al uso y difusión de dicha información, que además se sirven de la creación de entidades que tendrán por objeto principalmente el cumplimiento de las normas destinadas a regular esa materia, así como también, existen ordenamientos más permisivos y que únicamente intervienen en aquellos casos en los cuales ya existe una vulneración al derecho a la privacidad de los usuarios. Pero, lo anterior no debe ser visto únicamente como un retraso jurisdiccional por parte de la legislación colombiana, sino que, está situación expone una oportunidad para la misma pues trae consigo ejemplos de legislaciones funcionales que brindan herramientas para combatir los problemas relacionados al tema, además de servir por sí misma como elemento de información, permitiendo realizar un análisis de jurisprudencia comparada que permita sacar lo mejor de cada una de estas normas con la intención de llegar a una posible evolución legislativa en materia de protección de datos en Colombia.

En cuanto al impacto jurídico de la aparición de las cookies publicitarias y el peligro que representan a la seguridad de los datos, se debe reconocer que tanto a nivel nacional como internacional, el derecho a través de los distintos ordenamientos jurídicos ha hecho presencia en el tema de la regulación de las bases de datos que almacenan datos personales de los usuarios en línea, por lo tanto, dicha regulación es aplicable a las cookies y se ha manifestado tanto de forma regulatoria, procedimental y sancionatoria, encontrando que aunque la jurisprudencia colombiana en materia de hábeas data es limitada en comparación con otros

países, se ha adaptado un sistema pertinente que obedece al menos a regular los supuestos mínimos que pueden acontecer en relación con la obtención de datos personales a través de distintas herramientas como pueden ser las cookies.

BIBLIOGRAFÍA

- Becerra, J., Cotino-Hueso, L., León, I. P., Sánchez-Acevedo, M. E., Torres-Ávila, J., & Velandia-Vega, J. (2018), El big data en la ciberdefensa y la ciberseguridad nacional versus el derecho a la privacidad del ciudadano colombiano. Editorial Universidad Católica de Colombia, Bogotá, Colombia.
- S. E., & D. C. (2018). Protección de datos personales en los servicios de internet. Universidad Católica de Colombia.
- Chen Mok, S., (2010), Privacidad y protección de datos: un análisis de legislación comparada. Diálogos Rev. electr. hist vol.11 n.1 San Pedro Aug. 2010
- Colombia, Corte Constitucional (1991) Constitución Política de Colombia.
- Ducuara Cuervo, C. & Soto Espinoza, (2018) PROTECCIÓN DE DATOS PERSONALES EN LOS SERVICIOS DE INTERNET. Bogotá, Colombia.
- Flaquer Riutort, J. (2021), LA FUNCIÓN PUBLICITARIA DE LAS COOKIES: MECANISMOS DE PREVENCIÓN Y CAUTELA EN EL DERECHO ESPAÑOL. (THĒMIS-Revista de Derecho) Universitat de les Illes Balears, Mallorca, España.
- Fernández, E, M. L. (2001) INTERNET Y LOS DERECHOS FUNDAMENTALES. Universidad Autónoma de Madrid, Madrid, España.
- Galvis Cano, L. (2012), PROTECCIÓN DE DATOS EN COLOMBIA, AVANCES Y RETOS (revista LEBRET) Universidad Santo Tomás, Bogotá, Colombia.
- Londoño Congote, A, (2021), Tratamiento de datos personales a través de web cookies: análisis bajo la legislación colombiana de protección de datos personales. Universidad de los Andes, Bogotá, Colombia
- Maqueo Ramírez, M.S, Gonzales, G.M, Gayo, M.R (2017) Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. Rev. Derecho (Valdivia) vol.30, Chile.
- Mendoza Galindo, L.F (2018) Derecho a la intimidad, privacidad y autorregulación informática en el ámbito de aplicación de la ley 1581 de 2012. Universidad Católica de Colombia, Bogotá, Colombia.
- Peláez, H. & Riascos, A. (2020). La protección de datos personales y la privacidad en Internet. El caso de Colombia. Working Paper FSCC, Volumen 1.
- Remolina, A, N. (2013) Tratamiento de datos personales: Aproximación internacional y comentarios a la ley 1581 de 2012. (LEGIS) Colombia,
- Ruiz, J. C. (2020). Análisis monográfico de la protección de datos personales en Colombia. Universidad Nacional Abierta.
- R, (2007) El derecho fundamental a la protección de datos: perspectivas. Revista de los Estudios de Derecho y Ciencia Política de la UOC, Catalunya, España.
- Vásquez Vélez, A. (2021). El ámbito de aplicación del régimen jurídico colombiano

para la protección de datos personales. Su alcance frente a empresas extranjeras sin representación jurídica en Colombia. Universidad Javeriana, Bogotá, Colombia.

- Ruiz, J. C. (2020). Análisis monográfico de la protección de datos personales en Colombia. Universidad Nacional Abierta.