"DATOS PERSONALES, ACTIVOS DIGITALES"

Nicolás Obando Ruiz

Sergio Cock Vasquez

UNIVERSIDAD EAFIT

ESCUELA DE DERECHO

MEDELLÍN

2016

NICOLAS OBANDO RUIZ
SERGIO COCK VASQUEZ
Monografía presentada para optar al título de Abogado

Asesora
MARIA ISABEL RUIZ JIMENEZ

UNIVERSIDAD EAFIT
ESCUELA DE DERECHO
MEDELLÍN
2016

Nota de aceptación

_____

_____

_____

_____

_____

_____

Firma del jurado

_____

Firma del jurado

MEDELLÍN, 2 DE MARZO DE 2016

CONTENIDO

Pág

INTRODUCCION 6

RESUMEN 10

1. MARCO NORMATIVO 12

1.1. REGIMEN DE PROTECCION DE DATOS PERSONALES 12

1.2. ESTATUTO DEL CONSUMIDOR 23

1.3. CODIGO COLOMBIANO DE AUTORREGULACION PUBLICITARIA 28

2. JURISPRUDENCIA 39

2.1. SENTENCIA C-748 DE 2011 39

2.2. RECONSTRUCCIÓN HISTORICA 43

3. NORMAS DE DERECHO COMPARADO 50

3.1. UNIÓN EUROPA 50

3.1.1. REGLAMENTO NO. 45/2001 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 18 DE DICIEMBRE DE 2000 50

3.1.2 DIRECTIVA 2009/136/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 25 DE NOVIEMBRE DE 2009 53

3.2. ESTADOS UNIDOS 58
3.3. TERRITORIALIDAD DE LA LEY 61

4. POLÍTICAS DE GOOGLE EN TRATAMIENTO DE DATOS PERSONALES Y PUBLICIDAD 66

5. MODELOS DE PUBLICIDAD DIGITAL 71

6. FUTURO PROYECCIÓN DEL MERCADO Y LEGISLACIÓN 82

7. BIBLIOGRAFIA 87

INTRODUCCIÓN

El derecho como un mecanismo de regulación de las actividades humanas vive en un reto constante de mantenerse vigente. Así como en algunas ocasiones las normas tratan de dirigir la conducta de los ciudadanos antes de que estos mismos comiencen a realizar dichas actividades, existen situaciones en las cuales son las normas las que aparecen en una etapa posterior. En estos casos los retos no sólo se basan en direccionar esas actividades humanas sino en entenderlas y en crear una relación articulada con el sistema jurídico.

Es indiscutible que el internet ha causado una revolución en la forma como viven los seres humanos actualmente. El tiempo que permanecen las personas en línea es cada vez mayor, y es más el número de personas conectadas en diversas plataformas. La inversión que hacen las empresas para llegar a las audiencias que se encuentran conectadas a estas plataformas aumenta de una forma exponencial llegando al punto de utilizar los datos personales, información de los individuos, para hacer una publicidad más acertada, con más efectividad hacia el usuario final. La publicidad digital y los datos personales son dos conceptos que han adquirido una significativa relevancia en los últimos años. Estrategias como la compra programática de audiencias, Big Data, instalación de cookies en los navegadores, email marketing, adwords, socialmedia, networking e influenciadores han aparecido en el mercado publicitario como una competencia a los medios tradicionales.

El mundo de la publicidad digital se vuelve relevante en la medida en que permite perfilar audiencias. Los anunciantes están ahorrando dinero al llegarles a sus públicos

objetivos de forma separada e individualizada. A diferencia de la televisión, radio y prensa, los medios modernos permiten escoger a quién se le quiere enviar el anuncio publicitario. A través de estos medios se pueden hacer segmentaciones por género, nombre, edad, fecha de cumpleaños, gustos y preferencias, lugar donde vive, profesión, familiares, amigos y cuantos datos personales sean relevantes para una campaña publicitaria efectiva.

Radio, prensa, vallas, volantes y televisión fueron medios tradicionales y predominantes del siglo XX, estos eran los principales actores del mercado publicitario cuando la oferta era más limitada que la demanda. Hoy en día, siguen con gran participación del mercado, sin embargo, las plataformas digitales surgen como un fuerte competidor proporcionando analíticas más acertadas que los medios tradicionales cuyas herramientas no son tan precisas.

Los medios tradicionales utilizan herramientas como Ibope[1], EGM[2], TGI[3] para las mediciones de sus audiencias. Estas, son principalmente encuestas representativas que hacen mediciones en distintos sectores demográficos de las principales ciudades del país para determinar, basado en la estadística, cuál es el perfil de las audiencias de estos medios. En otras palabras, a modo ilustrativo, con 1200 encuestas se puede determinar

[1] **Ibope:** Produce información de medición de audiencia para canales y programadores de televisión. IBOPE Media Colombia. Disponible en: www.Ibope.com/medios.html

[2] **EGM:** Estudio General de Medios estudio poblacional que busca una representación adecuada del universo objetivo, a través de una muestra interrogada acerca de su comportamiento en relación al consumo de medios entre otras cosas. ACIM Colombia. Disponible en: http://www.acimcolombia.com/estudios/estudio-general-de-medios-egm/

[3] **TGI:** Target Group Index es una herramienta de análisis para facilitar la toma de decisiones estratégicas que abarca hábitos de comportamiento y consumo de medios y de productos. IBOPE Media Colombia. Disponible en: www.Ibope.com/medios.html

cuál es la emisora más escuchada en el Valle de Aburrá. Un proceso muy parecido a lo que ocurre cuando se realizan encuestas para predecir quién será el próximo gobernante.

En los medios digitales, por su parte, no solo se mide cada momento en el que existe una interacción con audiencias, sino que como se explicó anteriormente, permiten saber quiénes son las personas con las que se está interactuando. Cuando un usuario llena información en Facebook, cuando se hace una búsqueda en Google, cuando comienza a seguir otra cuenta en twitter, o llena su perfil profesional en Linked In, no solo está interactuando en la red, sino que está entregando información personal como: dónde trabaja, dónde vive, cuáles son sus gustos, etc. Esto abre un abanico de posibilidades comerciales para muchas empresas, pero también ha logrado captar la atención de los entes reguladores, los cuales llegan en una etapa posterior a estos procesos de innovación disruptiva[4].

En una actividad humana en la cual no solo se abordan situaciones jurídicas típicas del estatuto del consumidor, sino que se conjugan situaciones jurídicas tales como la de tratamiento de datos personales y especialmente datos personales sensibles, donde el derecho fundamental a la intimidad establecido en el artículo 15 de la Constitución es llamado al campo de acción, cabe hacerse la pregunta de ¿cuál es el límite en el que la publicidad digital que trata con datos personales de los individuos puede operar legalmente, respetando los preceptos normativos y las buenas prácticas establecidas en el ordenamiento jurídico Colombiano?

[4] **Innovación Disruptiva:** Clayton Christensen (profesor en Harvard Business School) Se refiere a cómo puede un producto o servicio que en sus orígenes nace como algo residual o como una simple aplicación sin muchos seguidores o usuarios convertirse en poco tiempo en el producto o servicio líder del mercado. http://www.luisan.net/blog/marketing/innovacion-disruptiva

El objetivo de esta monografía es permitirle al lector no experto en materia jurídica o publicitaria entender de forma clara e ilustrativa, cual es el panorama jurídico en Colombia con respecto al uso de los datos personales de las personas en estrategias comerciales y publicitarias. En este sentido se va a hacer una descripción de todas las herramientas jurídicas existentes, tanto a nivel nacional como internacional en Europa y Estados Unidos. Luego, abordar de forma ilustrativa y descriptiva cuáles son los tipos de estrategias publicitarias y comerciales y destacar en qué casos sí hay uso de datos personales y en cuáles no. Concluyendo con una breve exposición de los retos que enfrenta el Estado en el mediano plazo, y una postura de los autores sobre cómo abordar aquellas dificultades.

RESUMEN

Los datos personales considerados como activos digitales hacen referencia a un fenómeno que se viene presentando cada vez con más frecuencia. Empresas como Facebook, Google, Twitter, se han convertido en expertos en la recolección de información personal de sus usuarios. Todo el esfuerzo y recursos invertidos en lograr recopilar la mayor cantidad de información y de la forma más precisa cumple un objetivo principal, este es, vendérselo a los anunciantes que están buscando publicitar sus marcas y productos ante el público consumidor. Es de este modo que saber qué quieren las personas, y convertirse en un puente entre los anunciantes y los usuarios es lo que en este texto se denomina tener un activo digital, activos que para el caso de Google representaron 67.39 billones de dólares[5] y 17.079 billones de dólares para Facebook[6]. El objetivo de esta monografía es permitirle al lector no experto en materia jurídica o publicitaria entender de forma clara e ilustrativa, cuál es el panorama jurídico en Colombia con respecto al uso de los datos personales de las personas en estrategias comerciales y publicitarias. En este sentido se va a hacer una descripción de todas las herramientas jurídicas existentes, tanto a nivel nacional como internacional. Luego abordar de forma ilustrativa y descriptiva cuáles son los tipos de estrategias publicitarias y comerciales, y destacar en qué casos sí hay uso de datos personales y en

[5] Statista. The Statistics Portal. Disponible en: http://www.statista.com/statistics/266249/advertising-revenue-of-Google/ Tomado el 21 de febrero de 2016

[6] Statista. The Statistics Portal. Disponible en: http://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/ Tomado el 21 de febrero de 2016

cuáles no. Para concluir con una breve exposición de los retos que enfrenta el Estado en el mediano plazo, y una postura del autor sobre cómo abordar aquellas dificultades.

1. MARCO NORMATIVO DE LA PUBLICIDAD E INFORMACION POR MEDIOS DIGITALES

1.1. RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES

El régimen de protección de datos personales aparece como una necesidad y respuesta ante la tendencia en los hábitos de consumo de productos y servicios digitales de los individuos en la actualidad. A medida que la tecnología va evolucionando, los seres humanos se acogen a las soluciones que ésta brinda y son más las horas que pasan frente a dispositivos conectados en línea. La información que un individuo puede estar publicando en línea, sea consciente o inconscientemente, es abundante. Este es uno de los hechos que motivó que el Congreso de Colombia, por medio del acto legislativo No. 2 de 2003 tomara cartas en el asunto expidiendo un mandato de optimización a los órganos Estatales el cual materializa el texto del artículo 15 de la Constitución Política de Colombia.

> **Artículo 15**. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden

> ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley…[7]

Del texto anterior, es necesario destacar el punto que hace mención al derecho que tienen las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas, esto es habeas data. Igualmente debe destacarse el derecho a la intimidad y como aquella que protege los datos personales. La razón por la cual se destaca, es porque este es el punto de partida de todo lo que conforma y constituye el régimen de protección de datos personales, los cuales se han vuelto más fáciles de recolectar, detallados, e íntimos en la medida en que los desarrollos tecnológicos han ido avanzando. Todo esto para concluir y afirmar que la digitalización ha ido conquistando un mayor terreno en la vida de las personas.

El 17 de octubre de 2012 se sancionó la Ley Estatutaria 1581 de 2012, ley por medio de la cual se dictaron disposiciones generales para la protección de datos personales. El objetivo principal por el cual se creó esta ley fue para el desarrollo del derecho constitucional consagrado en el artículo 15 de la Constitución Política. Entre muchas figuras novedosas que surgieron de esta ley cabe resaltar el derecho de habeas data, el que tienen los individuos para conocer, actualizar y rectificar la información que de ellos exista en bases de datos. Esta ley estatutaria entra a operar como pilar de todo el régimen de protección de datos personales en Colombia.

[7] Secretaria de Senado. "ACTO LEGISLATIVO No. 2 DE 2003"., 2003. Web. 15 Feb. 2016. Congreso de la República de Colombia.

Los principios que rigen el régimen de protección de datos personales son los siguientes.

a) **Principio de legalidad en materia de Tratamiento de datos:** El tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;

b) **Principio de finalidad:** El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;

c) **Principio de libertad:** El tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;

d) **Principio de veracidad o calidad:** La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error;

e) **Principio de transparencia:** En el tratamiento debe garantizarse el derecho del titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin

restricciones, información acerca de la existencia de datos que le conciernan;

f) **Principio de acceso y circulación restringida:** El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley;

Los datos personales, salvo la información pública, no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la presente ley;

g) **Principio de seguridad:** La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

h) **Principio de confidencialidad:** Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la

> información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma. [8]

Con base en los principios anteriormente expuestos, surgen una serie de derechos en favor de los titulares de los datos personales. Cualquier persona titular de datos personales puede exigir al responsable de la administración de la base de datos que le deje conocer los datos que de él o ella se dispongan; puede exigir que se actualicen y/o rectifiquen los datos; puede solicitarle al administrador de los mismos que le muestre constancia de la autorización dada por él o ella para el tratamiento de su información personal; presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley; revocar la autorización, solicitar la supresión del dato; finalmente puede ser informado por el responsable del tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.

Del otro lado, aquellos sujetos, personas jurídicas y entidades estatales encargadas del tratamiento de datos personales les surgen una serie de deberes. Entre estos deberes se pueden identificar; garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data; informar al titular cuál es la finalidad de la recolección de los datos personales y cuáles son los derechos que le asisten; conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta,

[8] LEY ESTATUTARIA 1581 DE 2012. (2012). Por *Congreso de Colombia*. República de Colombia. tomado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html Tomado el 14 de febrero de 2016.

uso o acceso no autorizado o fraudulento; rectificar la información cuando sea incorrecta; exigir al Encargado directamente del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular; tramitar consultas y reclamos; adoptar manual interno de políticas y procedimiento para garantizar el cumplimiento de la ley; y cumplir con las instrucciones y requerimientos hechos por parte de la Superintendencia de Industria y Comercio.

La definición que trae la ley al concepto dato personal es "Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"[9]. Esta es una definición corta pero concreta, en el sentido que la dirección de residencia, la edad, fecha de cumpleaños, las páginas web a las que se ingresan, los videos que se descargan, las fotos en redes sociales a las cuales se les da "me gusta"[10] son datos personales de los cuales las empresas están obteniendo información sobre el perfil del usuario. Entre los distintos datos que puede llegar a entregar voluntariamente un individuo, la ley 1581 de 2012 creó adicionalmente las categorías especiales de datos personales.

Las categorías especiales se dividen en dos referencias; la primera, es la categoría de datos sensibles y, la segunda, es la categoría de los datos de los niños, niñas y adolescentes. En la ley estatutaria aparece la definición del concepto dato sensible en el artículo 5o.

[9] Ibid. Art. 3

[10] Expresión comúnmente utilizada en las redes sociales para demostrar identidad con algún elemento publicado en la plataforma.

> Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.[11]

La ley expresamente prohíbe el tratamiento de datos sensibles, salvo cuando el titular ha dado su autorización explícita, cuando el tratamiento sea necesario para salvaguardar la vida del titular y este se encuentra física o jurídicamente incapacitado y, por último, cuando estos datos sean necesarios para el reconocimiento de un derecho en un proceso judicial. Igualmente se prohíbe el tratamiento de los datos personales de los niños, niñas y adolescentes, salvo aquellos datos que sean de naturaleza pública. Adicionalmente, se hace un llamado a las entidades educativas y a los representantes legales de los niños para concientizar y enseñar sobre el uso y manejo responsable de sus datos personales.

No se deben pasar por alto dos elementos adicionales que trae la ley 1581 de 2012, estos son la autoridad competente y el Registro Nacional de Bases de Datos. El artículo 19 dice “La Superintendencia de Industria y Comercio, a través de una delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y

[11] Ibid. Art. 5

procedimientos previstos en la presente ley."[12] Clara y expresamente dejando a la Superintendencia de Industria y Comercio como el órgano facultado para tratar los asuntos que se puedan presentar sobre habeas data.

El registro nacional de bases de datos es una novedad que trae la ley 1581. Lo define como el directorio público de las bases de datos sujetas a tratamiento que actualmente están operando en el país. Es una plataforma prevista a ser de libre consulta, y les permitirá a los ciudadanos acceder libremente para consultar los datos que de ellos se tienen. Las empresas, personas jurídicas que se encuentren operando y tratando bases de datos tendrán la obligación de registrarlas ante el registro nacional de bases de datos.

El último punto que queda por destacar estipulado en la ley, es con respecto a la transferencia de datos a terceros países. El artículo 26 de la ley establece que se prohíbe la transferencia de datos personales de cualquier tipo, a países que no proporcionen niveles adecuados de protección de datos. Para efectos de la ley, se estableció que se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia.

Los efectos prácticos que surgen de lo anterior son bastante trascendentales debido a que afecta muchos tipos de situaciones comerciales que se encuentran operando en la actualidad. Estos efectos van desde la situación en la que se encuentran empresas

[12]Ibid. Art. 19

colombianas que utilizan servicios en la nube o cloud computing[13] con servidores[14] en países no seguros para el almacenamiento de información corporativa como bases de datos de clientes, hasta lo que ocurre con empresas extranjeras provenientes de países no seguros, implementando estrategias comerciales y de publicidad digital en Colombia. Para las empresas colombianas surge la obligación de buscar proveedores que ofrezcan sus servicios en países que tengan políticas que para el Estado Colombiano sean suficientes para considerarlo un lugar seguro en tratamiento de datos personales.

Con respecto a lo anterior, es importante tener en cuenta la situación entre la Unión Europea y Estados Unidos acerca del Tratado de Puerto Seguro[15]. Lo importante para destacar de esta situación jurídica es que el Tribunal de Justicia Europeo decidió anular el Tratado de Puerto Seguro que permite a compañías transferir datos desde Europa a Estados Unidos, al considerar que los datos no están suficientemente protegidos por el país norteamericano. En otras palabras, Estados Unidos, el país con el cual Colombia

[13] **Nube, Cloud computing:** Técnicamente la nube, que viene del inglés *Cloud computing*, es el nombre que se le dio al procesamiento y almacenamiento masivo de datos en servidores que alojen la información del usuario. Disponible en: http://www.conexionbrando.com/1389864-que-es-la-nube-para-que-sirve-y-cuales-son-los-servicios-que-tenes-que-conocer. Tomado 1 de febrero de 2016.

[14] **Servidor:** Un servidor, como la misma palabra indica, es un ordenador o máquina informática que está al "servicio" de otras máquinas, ordenadores o personas llamadas clientes y que le suministran a estos, todo tipo de información. Estos aparatos suelen tener más capacidad tanto de almacenamiento de información como de memoria principal, ya que tienen que dar servicio a muchos dispositivos. Disponible en: http://aprenderaprogramar.com/index.php?option=com_attachments&task=download&id=487 . Tomado el 24 de diciembre de 2015.

[15] **Tratado de puerto seguro:** Estados miembros deben prever que la transferencia a un tercer país de datos personales únicamente pueda efectuarse cuando el tercer país de que se trate garantice un nivel de protección adecuado y cuando con anterioridad a la transferencia se respeten las disposiciones legales de los Estados miembros adoptadas con arreglo a las demás disposiciones de dicha Directiva; Disponible en: http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/common/B.12-cp--Decisi-oo-n--sobre-la-adecuaci-oo-n-conferida-por-los-principios-de-puerto-seguro.pdf. Tomado el 26 de diciembre de 2015

sostiene la mayor cantidad de interacciones en red, es considerado por la Unión Europea, como un país que no cumple con los parámetros suficientes para ofrecer un nivel adecuado de seguridad en el tratamiento de los datos personales.

Continuando con el Régimen de Protección de Datos personales colombiano, es necesario traer a colación el decreto reglamentario 1377 de 2013. En el artículo segundo, comienzan con una breve descripción de los datos personales tratados en ámbito doméstico. Explica que se excluyen de dicha ley y decreto, los datos almacenados en un ambiente personal y doméstico, este puede ser el caso, por ejemplo, de las grabaciones obtenidos por una cámara de seguridad en la casa de un individuo.

En el artículo tercero, definen los conceptos de Aviso de privacidad, dato público, datos sensibles, transferencia y transmisión. Sobre lo anterior es importante destacar el concepto de aviso de privacidad, ya que se tendrá en cuenta para un análisis posterior. Dice el decreto que el aviso de privacidad se entenderá bajo la definición de; ¨Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a [16]las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales. ¨

El capítulo segundo es referente a la autorización. De este se desprenden los artículos 4 al 12. Estos hablan sobre la recolección de los datos, la autorización, la autorización para casos de datos sensibles, el modo de obtener la autorización, la prueba, la

[16]

revocatoria de la autorización, datos anteriores al decreto, limitaciones temporales y requisitos especiales para el tratamiento de datos de menores.

Si bien cada uno de los puntos anteriores merece un análisis detenido, para la finalidad que persigue esta tesis, la cual tiene que ver con el uso de estos datos para fines publicitarios, se ahondara en el artículo séptimo, sobre el modo de obtener la autorización. Dice la norma que se entiende que la autorización es concedida cuando se ¨manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.

Si bien muchas plataformas obligan a los usuarios a aceptar sus términos y condiciones, inclusive antes de que puedan realizar la descarga de las mismas, existen otro tanto que permiten a los usuarios navegar libremente en sus páginas sin exigir o exhibirle al usuario los términos y condiciones sobre el uso de datos personales. Puede presentarse como una situación de análisis la contradicción entre las plataformas digitales que insertan cookies en los computadores de sus usuarios para obtener información personal de ellos, pero no les notifican expresamente que lo están haciendo, presumiendo que con tener los términos y condiciones publicados están cumpliendo con los requisitos legales. Esto, de cara a lo estipulado por la norma, de que el silencio no podrá asimilarse como una conducta inequívoca, plantea una situación interesante de cara a muchas páginas web que actualmente creen haber obtenido de forma correcta la información que están almacenando en sus bases de datos, cayendo en su gran mayoría en un error técnico y legal.

El capítulo tercero es sobre las políticas de tratamiento. En el artículo 13 establecen que los responsables de tratamiento de datos personales deberán desarrollar las políticas y velar por que los encargados para el tratamiento de las mismas las cumplan. Esta norma tuvo grandes implicaciones a nivel corporativo en Colombia, debido a que obligo a todas las empresas a construir sus propias políticas.

En los capítulos posteriores se abordan los temas sobre el ejercicio del derecho de los titulares, la transmisión y transferencia internacional de datos personales y la responsabilidad demostrada frente al tratamiento de datos personales.

El decreto 886 del 2014 es otro de los decretos reglamentarios expedidos en virtud de la ley 1581 de 2012. El objeto con el cual se expidió este decreto es reglamentar la información mínima que debe contener el Registro Nacional de Bases de Datos, así como los términos y condiciones bajo las cuales se deben inscribir en este los Responsables del Tratamiento. En él se define el ámbito de aplicación y se determina el plazo para la inscripción de las bases de datos por parte de los responsables.

1.2 ESTATUTO DEL CONSUMIDOR

¿Qué relación tiene el estatuto del consumidor con las políticas de tratamiento de datos personales con fines comerciales y publicitarios? En principio, se podría decir que no existe ninguna relación debido a que el estatuto del consumidor en ningún punto aborda el tema de tratamiento de datos personales de manera directa. Sin embargo, es importante tener en cuenta que la finalidad de esta monografía, es entender el panorama jurídico existente en Colombia, respecto al manejo de datos personales en relaciones

comerciales. Esto con el fin de abordar el tema de una manera más descriptiva que valorativa, pues en todo caso, las realidades comerciales siempre están un paso más adelante que las jurídicas. Ahora, esto no nos puede llevar a desconocer el papel regulador y protector del derecho. En este sentido, es importante analizar las etapas posteriores a las de las campañas publicitarias, y entender las posibilidades jurídicas de los usuarios que, a raíz de un manejo efectivo de su información personal, en el sentido de que se ejecuta una venta, han tomado la decisión de compra de un producto o servicio. Bajo esta lógica, el estatuto del consumidor se convierte en una herramienta jurídica que requiere ser analizada en esta tesis, debido a que está directamente relacionada al momento o situación en la que una persona está siendo abordada comercialmente por una compañía a través de una plataforma digital y se convierte en un instrumento posterior para la protección de los usuarios.

La combinación de ambas normas trae como consecuencia necesaria el análisis de algunas las situaciones que se pueden presentar en circunstancias donde convergen tanto el consumo o comercio electrónico como la publicación o exposición de datos personales por parte de los usuarios, los cuales podrían ser utilizados posteriormente, no necesariamente, a favor del consumidor o propietario de los datos personales.

Situaciones como la navegación cotidiana en internet o el comercio electrónico implica revelar una cantidad de información por parte del usuario que podrían ser de alta utilidad para los comerciantes, productores o proveedores. A travez de estos datos que pueden ser recopilado de una amplia variedad de mecanismos como los cookies, se puede llegar a predecir las necesidad, debilidades, intereses, gustos, hábitos y demás factores de decisión a la hora de comprar, los cuales podrían ser utilizados intencionalmente por parte del proveedor y/o productor para bienestar propio.

Una típica situación que se podría presentar es la utilización de necesidades o preferencias en las compras electrónicas, de tal forma que le permita al operador de la plataforma web sugerir la próxima compra del usuario de una manera precisa y fríamente calculada, de acuerdo a los comportamientos anteriormente plasmados en los sitios web. Por ejemplo, identificar los gustos del cliente a la hora de comprar prendas de vestir, una vez se realiza una transacción con uno de los elementos analizados, inmediatamente después sugerir un complemento a esa compra basada en los comportamientos expuestos anteriormente, tomando en cuenta, marcas, colores, estilos, rangos de preciso etc.

Otra situación, que se presenta usualmente en la navegación, es como los operadores de las plataformas web utilizan las búsquedas más recientes o habituales para sugerir productos y llamar la atención por medio de publicidad engañosa. Un claro ejemplo de esta práctica es cuando un usuario está buscando tiquetes aéreos para un destino particular pero no se concreta ninguna transacción. Luego, realizando otras actividades en internet se envían al usuario pop ups con publicidad engañosa, por ejemplo, tiquetes a Nueva York a 100 dólares, los cuales terminan siendo mucho más costosos.

En el capítulo VI se regula el tema de la protección al consumidor por medios electrónicos. Allí, se habla de los deberes del productor o expendedor como tal, y los deberes de estos en relación con el producto y la transacción, más no se menciona el tema central del trabajo, el manejo de los datos personales de los consumidores o usuarios de internet y las bases de datos que se configuran a partir de estos. Es de vital importancia mantener presente entonces los principios que se deben salvaguardar a la

hora de cotejar las situaciones donde se puedan vulnerar los derechos de los consumidores.[17]

Hay un eje central en las dos situaciones anteriores, el cual se sintetiza en la minería de datos. Esta práctica que cada vez es más común y utilizada por los comerciantes para conocer en detalle a sus clientes y poder establecer una estrecha relación con estos, tiene sus bemoles a la hora de hacer un análisis jurídico y proteccionista, donde se verán afectados, especialmente, derechos a la información e intimidad.

Cuando en una página web se recopilan datos de un usuario con fines legítimos y determinados, estos datos deben ser utilizados para ese fin específico de acuerdo al principio finalidad y libertad; finalidad, la cual debe ser informada al titular; libertad, pues el tratamiento de datos debe ser consentido previamente de manera expresa e informada. Al tener en cuenta el alcance estos dos principios es posible argumentar que no es posible realizar la minera de datos para situaciones donde lo único que se busque es el beneficio del operador de la página, pasando por encima del consentimiento del usuario y sus derechos. Pero, al fin y al cabo, la minería de datos siempre va a estar sujeta al alcance del consentimiento expreso, libre e informado que el usuario emita para el tratamiento de datos. Si se llega a comprobar que hay una práctica fuera de lo que el usuario expresamente autorizo esta seria claramente ilegitima.

En la segunda situación descrita anteriormente, hay un fenómeno el cual involucra la utilización de datos personales para eventualmente llamar la atención del cliente por medio de publicidad engañosa. Este tipo de publicidad se prohíbe en el Estatuto y esta prohibición se hace expresa en el artículo 30 de la ley 1480 de 2011. Esta misma ley, establece en el artículo 5to numeral 13, que la publicidad engañosa es “Aquella cuyo

[17] LEY 1480 DE 2011. (2011). Por *Congreso de Colombia*. República de Colombia. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html tomado el 28 de Diciembre de 2015.

mensaje no corresponda a la realidad o sea insuficiente, de manera que induzca o pueda inducir a error, engaño o confusión." En esta situación el tratamiento de datos es abiertamente ilegitimo, pues el fin con el cual se van a utilizar estos datos son fines abusivos, por lo cual no cabe la opción de considerarla como una práctica viable.

Diferente es la primera situación planteada en el supuesto donde todos, hipotéticamente, se benefician, tanto usuario o cliente, como proveedor o productor. En este primer caso se podría afirmar que es posible realizar minería de datos para fines benéficos de ambos extremos de la relación comercial, pero en aras de seguridad jurídica y protección al consumidor, que es el beneficiado en el estatuto del consumidor y al cual se le da prevalencia en la relación jurídica, por más benéfica que sea el fin del tratamiento de datos, este debe cumplir los requisitos de legalidad, y los principios anteriormente expuesto, es decir, independientemente del fin, debe haber un consentimiento expreso, claro, informado, con fines legítimos y previo al tratamiento de los datos.

En cuanto al recurso de retracto este no sería el mecanismo idóneo para proteger los datos personales, pues la naturaleza de este recurso lo que pretende es reestablecer el estado de cosas a una etapa posterior a la transacción realizada, es decir, un consumidor desea deshacer la compra que realizo sin tener que dar justificación alguna, obteniendo el dinero devuelto y devolviendo el producto que se haya recibido. Y es diferente deshacer una transacción a proteger los datos personales recopilados por un operador de una plataforma virtual.

Para la protección de los datos personales esta la revocatoria, uno de los derechos que tiene el titular de los datos personales. Este derecho se enuncia en el artículo 8, literal e) de la ley 1581 de 2012.

El Titular de los datos personales tendrá los siguientes derechos:

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

El ejercicio de este derecho seria el mecanismo ideal para poder sancionar al Encargado de los datos y obligar a estos a suprimir o eliminar los datos de la base de datos por su mal uso.

1.3 **CÓDIGO COLOMBIANO DE AUTORREGULACIÓN PUBLICITARIA**

Una de las herramientas en el ámbito jurídico colombiano que hace parte del marco normativo es el Código Colombiano de Autorregulación Publicitaria. La última actualización de dicho Código se realizó en octubre del 2013. Es importante resaltar los resultados que se han alcanzado a través del tiempo en lo que tiene que ver con las buenas prácticas del oficio y cómo los actores de dicho gremio han acudido a la autorregulación como un mecanismo donde se demuestra la madurez y responsabilidad del gremio. Vale la pena citar un fragmento de la introducción donde se plantean las intenciones o el espíritu del Código en cuestión.

Los límites entre la labor del Estado y el que hacer de los particulares se han desdibujado abriendo la posibilidad

> para la interacción y la colaboración entre ambos actores de la sociedad contemporánea: la cosa pública y el interés común son tema de todos independientemente del sector económico, político o social y ello supone un esfuerzo colectivo y un trabajo en equipo en el que, desde las distintas perspectivas, todos aporten en el establecimiento de una mejor realidad. El Estado ha venido perdiendo su papel de policía y la sociedad civil ha asumido la responsabilidad que le corresponde a través de un ejercicio de conciencia propio y no impuesto por la fuerza.
>
> La regulación, esa práctica consistente en someter a reglas y a controlar en virtud del poder del Estado, viene dando paso a la autorregulación que es la elección voluntaria, producto del desarrollo, la madurez y la responsabilidad, de limitaciones en el ejercicio de la libertad.[18]

Desde 1980 cuando Colombia tuvo su primer Código de Autorregulación Publicitaria se han ido desarrollando los respectivos ajustes para enfrentar un mundo globalizado con nuevas prácticas y tecnologías.

Además, este Código, que es la expresión de la voluntad privada, en un intento de lo que deberían ser las prácticas publicitarias, como se establece en el artículo primero del Código, está guiado por los parámetros del Código de la Cámara de Comercio Internacional en la materia.

> La autorregulación ética en general, y la publicitaria en particular, ha sido y es sin duda una ardua labor no solamente por la adopción

[18] TAPIAS DELPORTE, X., & TRUJILLO TAMAYO, M. (2013). Unión Colombiana de Empresas Publicitarias UCEP. Unión Colombiana de Empresas Publicitarias UCEP., Disponible en http://www.ucepcol.com/#!codigoautorregulacion/c4fn. Tomado el 15 febrero 2016

> voluntaria de restricciones sino por la tentación de apartarse de su camino por las diversas circunstancias de competencia que se enfrentan permanentemente; su existencia es sintomática de un grado avanzado de desarrollo democrático y de la presencia de una industria madura, consciente de su responsabilidad social. Es también la prueba fehaciente de que, a pesar de los intentos por desvirtuar su importancia, es un mecanismo destinado a regir la conducta humana, más que por el castigo, por la conciencia de la buena fe y del respeto por los demás.[19]

Una de las actualizaciones que se realizó en este nuevo Código, y el cual es el punto central de esta monografía, es un capítulo completo sobre las nuevas tecnologías, en especial la publicidad en medios digitales interactivos. Antes de empezar a esgrimir el núcleo del tema digital, es pertinente hacer referencia tanto a los principios éticos que rigen dicho código como a las definiciones de algunos conceptos de alta relevancia que se establecen en él, pues, al fin y al cabo, son los principios que rigen la actividad para los agentes que se vinculen al ejercicio de la misma.

Principios Éticos de la Publicidad en Colombia

VERACIDAD: El mensaje publicitario debe atenerse a la verdad en relación con el producto anunciado y con los de la competencia, con el fin de evitar la confusión y de preservar la confianza del público en la actividad publicitaria.

[19]Ibid. Pg. 10

DECENCIA: Los mensajes publicitarios deberán respetar la dignidad de las personas, de las instituciones, de las autoridades legítimamente constituidas y de los símbolos patrios.

HONESTIDAD Y BUENA FE: En los mensajes publicitarios se respetarán estrictamente los principios de honestidad y buena fe en relación con lo que se afirma o transmite, tanto frente a los productos anunciados, como con los de terceros, sean o no competidores.

RESPONSABILIDAD SOCIAL: Los mensajes comerciales deben ser preparados de manera que contribuyan con el mejoramiento social, económico y ambiental del país, sin perjuicio de su objetivo esencial. En desarrollo de este principio los mensajes apelarán preferentemente a actitudes o sentimientos positivos y no podrán alentar o propiciar ninguna forma de discriminación, explotar injustificadamente el infortunio o el sufrimiento, aprovecharse del miedo, ni utilizar o dar la impresión de justificar, permitir o incitar una conducta violenta, ilegal o antisocial.[20]

Definiciones Importantes

[20] Ibid. Pg. 14

Del artículo 6to del Código de Autorregulación Publicitaria de Colombia se pueden extraer las definiciones de los conceptos de mayor relevancia para la aplicación del Código y su completo entendimiento.

ANUNCIANTE: Hace referencia a las personas naturales o jurídicas, en cuyo nombre se publican o difunden mensajes comerciales o se realizan actividades publicitarias.

CONSUMIDOR: Es toda persona natural o jurídica a la que se dirige el mensaje publicitario en buscando que conozca, adquiera, disfrute o utilice un determinado bien, servicio, idea, marca o empresa, ya sea como usuario final o como cliente o usuario comercial.

COMUNICACIÓN PUBLICITARIA: Es una comunicación de masas en la que el agente emisor destina un mensaje a un gran volumen de personas mediante los soportes denominados “mass-media”.

EMPRESA PUBLICITARIA: Toda persona natural o jurídica cuyo principal objetivo sea la prestación de servicios publicitarios.

MENSAJE COMERCIAL: Es cualquier forma de anuncio o publicidad elaborado para ofrecer al público productos con el objeto de promover su aceptación a través de los diferentes medios de comunicación y de difusión. Su concepto debe ser entendido en sentido amplio, comprensivo de cualquier forma de comunicación producida directamente por o en favor de anunciantes, con la finalidad principal de promover productos, servicios o ideas, o influir en el comportamiento del consumidor. Incluye cualquier técnica publicitaria como promociones, patrocinios y mercadotecnia directa.

MEDIOS DE COMUNICACIÓN: Es el instrumento o vehículo a través del cual se difunden o se hacen llegar al consumidor los mensajes comerciales, tales como prensa, televisión, radio, fax, teléfono, publicidad exterior, películas, medios digitales interactivos, correo directo, correo electrónico, etc.

MEDIOS DIGITALES INTERACTIVOS: Se refiere a cualquier plataforma, servicio o función que permita la comunicación electrónica vía internet o redes de comunicación electrónica. Incluye los servicios electrónicos a través de teléfonos celulares, los blogs, las revistas virtuales, las versiones digitales y audiovisuales de los medios impresos, páginas web de divulgación y difusión artística, emisoras de radio virtuales, entre otros, asistente digital personal y consolas de juegos interactivos que permiten a la parte receptora interactuar con la plataforma, servicio o función.

PRODUCTO: Es el bien o servicio sobre el que recae la publicidad.

Una vez están establecidos dichos principios y se tiene una claridad sobre algunos conceptos, hay que mirar el capítulo que se dedicó a los medios digitales interactivos. Cuando se analizan las prácticas publicitarias en los medios digitales hay múltiples temas que analizar. El primero de ellos, se establece en el artículo 50 del Código. Allí, se desarrollan los mensajes comerciales digitales individuales, mensajes que pretenden contactar al destinatario de manera directa y personal, por medio de correo electrónico, celulares o medios similares.

La primera condición que se impone a este tipo de mensajes es un encabezado en el cual se establezca de manera clara e inequívoca que el mensaje es de tipo comercial.

El envío de este tipo mensajes debe estar previamente autorizado por el destinatario y solo hay dos ocasiones en las que se permite enviar estos mensajes sin previa autorización; la primera, que existan bases razonables de que el destinatario pueda tener interés en el asunto del mensaje; y dos, cuando se establezca un mecanismo claro donde se pueda expresar el deseo de no volver a recibir otras comunicaciones en el futuro.

El fenómeno que ha surgido a partir de la posibilidad de enviar o suministrar información directamente a la persona que se quiere impactar con la información de manera individual a través de los medios electrónicos ha revolucionado el mundo y así el comercio y la forma de llegar a un público objetivo. Dice, además, el parágrafo del artículo citado del Código de Autorregulación Publicitaria que la publicidad nunca debe obstaculizar el uso normal que realiza el consumidor de los medios digitales interactivos.

Otro de los grandes temas tratados, del cual surgen numerosas controversias, está basado en los hábitos de navegación de usuarios de internet. Desde el desarrollo del internet, las compañías han utilizado toda la información que es posible recopilar en internet sobre los gustos, hábitos, tendencias y comportamiento de las personas para poder ser más eficientes y eficaces a la hora de planear una estrategia comercial. Este es un tema de alta sensibilidad, debido a la estrecha relación que tiene con la intimidad de las personas. Hoy en día, en un mundo digital como en el que se vive, es posible saber mucha más información de una persona de lo que antes era posible.

Dentro de las áreas que se pueden identificar están los grupos sociales de los que se rodea, los artistas que le gustan, los lugares que visita, las búsquedas que realiza en internet, las compras realizadas, las finanzas, identificar sus familiares, relaciones

afectivas, etc. Es por esto que toda esta información tan completa y compleja es de alto valor e importancia para una compañía pues le permite entender al consumidor, saber cómo está la compañía frente a ese consumidor y a partir de allí, identificar fortalezas y debilidades.

Los hábitos de navegación permiten a una compañía publicitaria segmentarlo y enviar mensajes comerciales de acuerdo a los intereses de las personas. Es así cómo se logra obtener con certeza lo que el consumidor quiere y como la compañía publicitaria puede ponerle una solución en la pantalla. Dice el artículo 53, en el que se regulan los mensajes comerciales en línea basados en hábitos de navegación de usuarios de internet(MBHU)[21], que en esta categoría de publicidad no se incluyen las actividades de operadores de sitios web, el envío cuantitativo de mensajes, los reportes cuantitativos de mensajes, ni la publicidad basada en el contenido de la página web que es visitada. La primera condición que requiere este tipo de publicidad es el consentimiento explícito del usuario antes de la recopilación y uso de los datos de sus hábitos de visita y navegación.

[21] Código Consolidado De Prácticas Publicitarias y Mercadotecnia de la Cámara de Comercio Internacional. El término "MBHU" se refiere a la práctica de obtener información respecto de las actividades en línea de los usuarios de una herramienta específica, en un periodo de tiempo, respecto de diferentes sitios web no afiliados para crear segmentos de interés, o para identificar tales hábitos de visita con los segmentos de interés, a fin de enviar mensajes relacionados con los intereses y preferencias del usuario web. MBHU no incluye las actividades de operadores de sitios web, el envío cuantitativo de mensajes, los reportes cuantitativos de mensajes, ni publicidad orientada a contenido (por ejemplo, publicidad basada en el contenido de la página web que es visitada; la visita actual de un consumidor a una página web; o la búsqueda de una respuesta). En el contexto de MBHU el término "tercero" se refiere a una entidad que realiza actividades relacionadas con "MBHU" en un sitio web no afiliado. Esto contrasta con un "operador de sitio web" o "first party" que es el dueño, controlador u operador del sitio web, incluyendo los sitios afiliados, con los cuales el usuario web interactúa. Disponible en http://www.codescentre.com/media/1328/cdigo%20consolidado%20icc%20(1).pdf . Tomado el 23 de enero de 2016.

Otra garantía que se pretende dar a los usuarios de las páginas web es una información clara y contundente que tanto los operadores del servicio publicitario, como los operadores del sitio web que monitorean los comportamientos deben publicar en sus sitios web sus prácticas de recopilación y uso de esta. Esta notificación informativa debe establecer el tipo de información recopilada y para qué será utilizada. En caso de que el usuario no esté de acuerdo en suministrar esa información se le debe brindar un mecanismo donde puedan plasmar su derecho de elección.

En el código de autorregulación publicitaria colombiano el artículo 54 habla de la publicidad en la world wide web, y establece claramente que toda publicación que aparezca durante la navegación debe permitir salir del mensaje y regresar a la página donde este salió por primera vez.

Otro de los temas interesantes tiene que ver con el manejo de las cookies. Las cookies o galletas inteligentes están inmersas en el uso diario del internet. Se utilizan de muchísimas formas, desde el carro de compras en las páginas de internet, hasta las configuraciones de presentación de las páginas. Las cookies son información enviada por un sitio web y almacenada en el navegador del usuario que le permita al sitio web consultar la actividad previa del usuario.[22] Uno de los problemas de las cookies es su alto nivel de interferencia con la privacidad del usuario, pues a través de esta se puede extraer gran cantidad de datos. Es por esta razón que el uso de cookies ha tenido un gran número de detractores.

[22] Techterms.com,. (2011). Definición de Cookie., Disponible en http://techterms.com/definition/cookie. Tomado el 15 febrero 2016.

En el artículo 55 del Código se establece la regulación de los *cookies* o mecanismos similares, aparte de dar una breve definición de lo que es una cookie y su funcionamiento, establece un tema sobre la privacidad bastante interesante. A continuación, se transcribe un segmento de dicho artículo. “Las cookies son pequeños ficheros de datos generados a través de instrucciones enviadas por los servidores web a los programas navegadores de los usuarios, y que se guardan en un directorio específico del terminal de aquéllos, con el objetivo de reunir información compilada por el propio fichero.”

Respecto al tema donde se involucran los usuarios y se relacionan los derechos de privacidad establece el Código lo siguiente,

> Deberá proveerse a los usuarios de información clara y comprensible sobre la presencia y la finalidad de las cookies u otros dispositivos o técnicas similares, poniendo a su disposición mecanismos sencillos y gratuitos para informarles sobre cómo desactivarlas. Asimismo, se avisará de forma clara cuándo queda imposibilitado el acceso o la utilización de un servicio interactivo por ser necesario el envío e instalación de cookies u otros dispositivos o técnicas similares en el terminal del usuario.

Este Código, como se dijo anteriormente, es una muestra importante del sector privado – no es la manifestación del poder público- donde se muestran un conjunto de ideas o tendencias de lo que deberían ser las normas aplicables a esta temática según estos sujetos. Se enuncia en el código que la autorregulación es una tendencia que ha venido reemplazando la regulación por parte del poder público, o más bien, supliendo unas

deficiencias en áreas de vacíos jurídicos por falta de eficiencia y capacidad operativa del sistema legislativo e incluso judicial.

Ahora bien, el hecho de que se constituyan códigos de autorregulación por parte de gremios, grupos o individuos y parte de la academia no reemplaza el poder legislativo constituido en el país, pues se estarían violando los principios democráticos más básicos que estructuran nuestro ordenamiento jurídico. Se cree que la manera más apropiada de abordar este código es desde una perspectiva crítica y constructiva pues puede ser un instrumento ilustrativo, guía, y donde se plasmen las ideas de algunos agentes los cuales pueden contribuir a la elaboración normativa por parte del órgano legislador, pero sin saltarse el proceso legislativo que legitima el ordenamiento sobre el cual nos pronunciamos. Esto implica que no existe una vinculación al código por parte de individuos que no se acojan a él o expresamente lo hagan parte de sus normas de regulación, algo así como un acuerdo por medio del cual se pacta que este código será una norma para las partes.

Otra de las perspectivas desde la cual se podría analizar el código, saliéndonos del ordenamiento jurídico colombiano, específicamente Estado Unidos de America, seria acudir a la figura allí denominada “best practices” las cuales son tenidas en cuenta en los juicios, pero en ningún caso, para el caso colombiano sustituiría la Ley, sino que más bien se constituirían como marcos de referencia a la hora de fallo.

2. JURISPRUDENCIA

2.1 SENTENCIA C-748 DE 2011

La Corte Constitucional en cabeza del magistrado Ponente Dr. Jorge Ignacio Pretelt Chaljub realizó la revisión de constitucionalidad del proyecto de ley Estatutaria No. 184/10 Senado, 046/10 Cámara. Por medio de un análisis extenso de todo el contenido normativo del proyecto de ley, además de la revisión formal y de vicios de procedimiento en su aprobación, queda como producto el aporte jurisprudencial de este órgano judicial. Es pertinente traer a esta monografía las consideraciones realizadas por la Corte con respecto a los enunciados en algunos de los artículos, debido a la implicación que esto puede llegar a traer para el tema que se está analizando en este trabajo. Esta sentencia es de alta importancia para el tema tratado, pues como lo establece Nelson Remolina Angarita, cuando uno lee la Ley Estatutaria 1581 de 2012 "…debe leerse de manera conjunta con la sentencia C-748 de 2011 pues la misma contiene precisiones sobre el texto aprobado por el Congreso de la República de Colombia. Estas líneas se refieren a algunos aspectos cardinales sobre la misma que serán relevantes en la interpretación y reglamentación de la ley en comento." Además, Remolina destaca algunos puntos de alta relevancia que juega esta sentencia dentro del ordenamiento jurídico colombiano y para ello hare referencia a la introducción de su texto.

> En primer lugar, por tratarse de una revisión automática e integral de todo el texto de la ley, la misma será el referente permanente para la interpretación del alcance de la ley; En segundo lugar, también será el punto de referencia que debe tener presente el gobierno nacional para la reglamentación de la ley y, en tercer lugar, la sentencia comprende una serie de precisiones y adiciones al texto de ley 1581 de 2012 aprobado por el Congreso. En otras palabras, la Corte modificó y precisó algunos tópicos de la ley, lo cual obliga a que hacia futuro la ley se lea y aplique de manera armónica con el texto de la sentencia en comento.[23]

La Corte se pronuncia con respecto al artículo 3 literal (a) sobre las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico como una de las excepciones a la aplicación de este régimen. En este punto se especificó la distinción que existe entre los datos que se tratan en un ambiente personal o doméstico contra los datos que se tratan en un ambiente interno. Luego de una consulta realizada por Asobancaria sobre la similitud entre ambos conceptos (los datos internos y los datos en un ambiente personal o doméstico), dice la Corte que es necesario entender la voluntad del legislador en el sentido que cuando se hace referencia a un ambiente personal o doméstico es porque hace referencia a personas naturales. Sobre esa posición asumida por la Corte y el legislador es necesario hacer una crítica, ya que no hace diferencia que sea una persona jurídica o una persona natural la que esté haciendo uso y

[23] **Nelson Remolina Angarita**. Profesor Asociado y Director del GECTI (Grupo de Estudios en internet, Comercio electrónico, Telecomunicaciones e Informática) de la Facultad de Derecho de la Universidad de los Andes. Fundador y director del observatorio de la protección de datos personales en Colombia. Miembro de la red habeasdata.org . Secretario Académico de la Red Académica Internacional de Protección de Datos. Disponible en http://www.rlpdp.com/2012/12/382/

tratamiento de los datos personales de un individuo, en la medida que ese individuo dueño de sus datos personales no pueda ejercer su derecho de hábeas data. En otras palabras, tiene tanto poder una persona natural desde la comodidad de su casa, como una persona jurídica con su equipo de trabajo, para hacer mal uso de la información personal.

Ahora bien, aunque la Corte deja el tema inconcluso en este sentido, pero a su vez es consciente de tal situación y aclarándolo en el párrafo citado,

> En consecuencia, una interpretación del inciso tercero del artículo 2 consonante con la Constitución y el contenido y finalidad del proyecto de ley es que aquél no prevé regímenes excluidos de la aplicación de la ley sino exceptuados de algunas de sus disposiciones en virtud de los intereses que se hallan en tensión. Esos casos exceptuados deben ser regulados por leyes estatutarias especiales y complementarias, las cuales deberán sujetarse a las exigencias del principio de proporcionalidad.
>
> En este orden de ideas, las leyes especiales que se ocupen de los ámbitos exceptuados deberán **(i)**perseguir una finalidad constitucional, **(ii)** prever medios idóneos para lograr tal objetivo, y **(iii)** establecer una regulación que, en aras de la finalidad perseguida, no sacrifique de manera irrazonable otros derechos constitucionales, particularmente el derecho al habeas data. Además, de conformidad con los principios que se examinarán más adelante, el cumplimiento de las garantías y la limitación del habeas data dentro de los límites de la proporcionalidad

> debe ser vigilada y controlada por un órgano independiente, bien sea común o sectorial.

Una de las ilustraciones más útiles que realiza la Corte en la sentencia mencionada anteriormente, tiene que ver con los tipos de modelos que existen en el mundo sobre la regulación de datos. Dice la Corte que existen básicamente dos modelos de protección de datos, uno centralizado y uno sectorial.

El primer modelo al que se hace referencia "parte de una categoría general de datos personales y de la idea que cualquier tratamiento de ellos es considerado per se potencialmente problemático," y es en consecuencia que "debe sujetarse a unos principios y garantías mínimas comunes, susceptibles de ser complementadas con regulaciones especiales -según el tipo de dato y los intereses involucrados, pero que de ninguna manera suponen una derogación de los estándares de protección generales".

Se complementa lo anteriormente expuesto con una característica muy propia del sistema centralizado, "la existencia de una entidad central, autónoma e independiente, que supervisa la instrumentación, cumplimiento normativo y ejecución de los estándares de protección generales, y que está facultada para autorizar o prohibir las transferencias de datos internacionales atendiendo a la equivalencia de la protección que ofrece el país de destino."

Por el otro lado, el modelo sectorial "no parte de una categoría común de datos personales y por ello no se considera que todos estos datos deban estar sometidos a la misma regulación mínima." De esto se desprende la justificación por la cual unos datos necesitan una protección especial y otros no. Esta protección se determina por la relación

que tienen estos datos con la intimidad. Además, para la protección de ciertos tipos de datos se tienen en cuenta conceptos como la seguridad y defensa nacional. En palabras de la Corte "la regulación sectorial se basa en una especie de ponderación de intereses que da lugar a reglas diferenciadas según el tipo de dato y que otorga más o menos poderes de intervención a las autoridades. La verificación del cumplimiento de las reglas también es asignada a autoridades sectoriales, las cuales son dotadas de distintos poderes de vigilancia y control, según el nivel de intervención previsto por el legislador."

Otro de los temas importante que toca este tipo de modelo sectorial es la idea de la "autorregulación de los mercados, razón por la cual el Estado solamente participa en la protección de ciertos datos en ámbitos en los que se presenta un alto riesgo de lesión de la intimidad, como la esfera financiera, la salud y los derechos de los niños."

2.2 RECONSTRUCCIÓN HISTORICA

Uno de los temas centrales que debemos mirar es el surgimiento de los derechos que se involucran en el tema desarrollado dentro de la monografía y para ello creemos pertinente hacer una aproximación y estudio de la historia de estos derechos. Tanto en la sentencia T-729 del 2002, magistrado ponente Eduardo Montealegre Lynett, como en la sentencia C-748 de 2011, magistrado ponente Jorge Ignacio Pretelt Chaljub, se hace referencia a las distinciones y contenidos de los derechos y su surgimiento en la historia. Para ilustrar al lector utilizaremos unas citas puntuales donde se narra los hechos históricos y los contenidos de estos derechos.

> Fue en Europa precisamente donde, con fundamento en esta última disposición y en vista de los riesgos a los que se enfrenta la intimidad en la sociedad de la información, comenzó a labrarse el camino para el reconocimiento del habeas data como un derecho fundamental autónomo. Así, en 1967, el Consejo de Europa convocó una comisión consultiva para estudiar los riesgos que las tecnologías de la información generan sobre los derechos de las personas. Como consecuencia de esta comisión, se expidió en 1968, la Resolución 509 sobre los derechos humanos y los nuevos logros científicos y técnicos, en la que se hizo un llamado a la protección de la privacidad frente a las nuevas tecnologías.[24]
>
> En 1983, una sentencia del Tribunal Constitucional alemán denominó por primera vez el derecho a la protección de los datos personales como derecho a la autodeterminación informativa, con fundamento en el derecho al libre desarrollo de la personalidad. Para este tribunal, tal derecho comprende la facultad de decidir por sí mismo cuando y dentro de qué límites procede revelar situaciones referentes a la propia vida. [25]

La comunidad europea ha estado al frente de la evolución de estos derechos y es en 1999 que "La configuración de la autodeterminación informativa como derecho autónomo culmina con la Carta de los Derechos Fundamentales de la Unión Europea"[26]

[24] Corte Constitucional. Sentencia C – 748 de 2011., (M.P.: JORGE IGNACIO PRETELT CHALJUB). p. 45.

[25] IBID, p. 47.

[26] IBID, p. 48.

Antes de pasar al plano nacional es importante tener claridad sobre una equivalencia conceptual. “En este sentido, derecho a la autodeterminación informática y derecho al habeas data, son nociones jurídicas equivalentes que comparten un mismo referente.” [27]

Al hacer una mirada al ordenamiento jurídico colombiano actual, fue

> …el artículo 15 de la Constitución de 1991 reconoció explícitamente el “(…) derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas” y además dispuso que “[e]n la recolección, tratamiento y circulación de datos se respetará la libertad y demás garantías consagradas en la Constitución”. Estos preceptos leídos en conjunto con la primera parte del mismo artículo 15 –sobre el derecho a la intimidad, el artículo 16 –que reconoce el derecho al libre desarrollo de la personalidad- y el artículo 20 –sobre el derecho a la información activo y pasivo y el derecho a la rectificación- de la Carta, han dado lugar al reconocimiento de un derecho fundamental autónomo catalogado como derecho al habeas data, y en algunas oportunidades, como derecho a la autodeterminación informativa o informática[28].

En este punto es importante retomar las distinciones interpretativas que tenía la Corte del derecho del habeas data. En un primer momento fue entendido como una garantía al derecho a la intimidad. En un segundo momento, se entendió tal derecho como una

[27] IBID, p. 47.
[28] IBID, p. 49.

manifestación del libre derecho de la personalidad. Como actualmente se acepta el concepto, y sería la tercera definición de tal derecho, es como un derecho fundamental autónomo.

Esta primera forma de utilizar el derecho del habeas data, vinculaba mucho la esfera privada de la persona y era visto como un campo impenetrable donde se incluía el proyecto de vida de la familia y el individuo y ni los particulares ni el Estado podían interferir en ella. La segunda línea de interpretación, hacía más énfasis en la autodeterminación y la libertad como un ámbito reconocido por el ordenamiento jurídico al sujeto. La tercera interpretación, la cual surge a partir del 1995 y se conserva hasta hoy, habla más del habeas data como un derecho autónomo donde su núcleo está compuesto por la autodeterminación informativa y la libertad[29]. Dice la sentencia C-748/11 "se está ante el nacimiento de un nuevo derecho, el de habeas data, en el que la privacidad no implica sencillamente la falta de información sobre nosotros por parte de los demás, sino más bien el control que tenemos sobre las informaciones que nos conciernen"[30].

Otro tema de vital importancia para la monografía es la diferenciación y delimitación sobre los derechos que surgen del artículo 15 de la constitución.

> …cobra especial importancia por tres razones: (i) por la posibilidad de obtener su protección judicial por vía de tutela de manera independiente; (ii) por la delimitación de los contextos materiales que

[29] IBID, p.50.
[30] IBID, p. 174.

> comprenden sus ámbitos jurídicos de protección; y (iii) por las particularidades del régimen jurídico aplicable y las diferentes reglas para resolver la eventual colisión con el derecho a la información[31].
>
> En la actualidad y a partir de los enunciados normativos del artículo 15 de la Constitución, la Corte Constitucional ha afirmado la existencia-validez de tres derechos fundamentales constitucionales autónomos: el derecho a la intimidad, el derecho al buen nombre y el derecho al habeas data. Sin embargo, el estado actual de cosas no fue siempre el mismo. El camino de la delimitación empieza en el año de 1994, con la sentencia T-229 de 1994, en la cual la Corte estableció una clara diferencia entre el derecho a la intimidad y el derecho al buen nombre. Más adelante, en el año de 1997, con la sentencia T-557 de 1997 la Corte precisó las diferencias entre el derecho a la intimidad y el habeas data, después de que la relación entre ambos se había manejado como de género a especie desde el año de 1992[32].

Una de las distinciones que se desarrolla en la sentencia C-748 de 2011 tiene que ver con la diferenciación entre el derecho a la información y el derecho del habeas data.

> Ciertamente, el derecho a la información, tanto en su dimensión activa y pasiva, es decir, el derecho a expresar y difundir información -incluidas las propias opiniones- y el derecho a recibir información veraz e imparcial, converge en algunos aspectos con el derecho al habeas

[31] Corte Constitucional. Sentencia T – 729 de 2002., (M.P.: EDUARDO MONTEALEGRE LYNETT).

[32] IBID, p. 7.

> data, en tanto, por ejemplo, (i) el derecho a la información puede recaer sobre datos personales y, (ii) en su faceta activa comprende el derecho a la rectificación que puede versar sobre datos personales. Sin embargo, el derecho a la información comprende todo tipo de datos, no solamente el dato personal, de ahí que deba concluirse que los dos derechos comprenden ámbitos de protección diferentes y que el proyecto de ley sujeto a revisión no desarrolla comprensivamente el derecho a la información[33].

Para ir finalizando y puntualizando lo que es y lo que implica el derecho del habeas data hay dos fragmentos que resumen concretamente lo que constituye este derecho y como se define este a su vez.

Al mirar el contenido del derecho de habeas data nos dice la Corte que algunas de las facultades que se le otorga al titular del derecho son;

(i) el derecho de las personas a **conocer** –acceso- la información que sobre ellas está recogida en bases de datos, lo que conlleva el acceso a las bases de datos donde se encuentra dicha información;

(ii) (ii) el derecho a **incluir** nuevos datos con el fin de que se provea una imagen completa del titular;

(iii) (iii) el derecho a **actualizar** la información, es decir, a poner al día el contenido de dichas bases de datos;

(iv) (iv) el derecho a que la información contenida en bases de datos sea **rectificada** o **corregida**, de tal manera que concuerde con la realidad;

[33]PRETELT, Op. Cit. P. 132

(v) (v) el derecho a **excluir** información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular –salvo las excepciones previstas en la normativa[34].

En conclusión, como se puede apreciar después de la reconstrucción realizada, el reconocimiento del derecho al habeas data busca la protección de los datos personales en un mundo globalizado donde la información y la informática cada día crece más. Esta protección obedece a la importancia que los datos implican para la garantía de otros derechos como la intimidad, el buen nombre y el libre desarrollo de la personalidad. Sin embargo, la estrecha relación con dichos derechos no implica que no exista una diferencia, pues es exigible su protección por medio de tutela y hay una serie de garantías diferenciables. Se toma entonces, el derecho del habeas data como un derecho fundamental y autónomo tanto en el plano nacional como internacional, el cual es exigible por cualquiera de los medios para proteger los derechos fundamentales.

Por último, encontramos en la jurisprudencia de mucha utilidad para entender los conceptos de la monografía una definición de lo que es el tratamiento de datos. Dice la Corte que el tratamiento de datos es,

> …es cualquier operación o conjunto de operaciones, sean o no automatizadas, que se apliquen a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión, y su proceso puede ser público o privado, requiriendo, en los términos de la jurisprudencia de esta Corporación, definiciones claras sobre el objeto o la actividad de las entidades administradoras de bases de datos, las

[34] IBID, p. 52.

regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos[35].

3 Normas de Derecho Extranjero

3.1 Unión Europa

Tiene relevancia mirar este conjunto de normas con relación al objetivo que se traza en este estudio, pues se puede afirmar que uno de los modelos o referentes a los cuales adhirió Colombia con la creación de la ley 1581, fue el europeo. Analizar cuáles pueden ser los límites al tratamiento de datos personales en el ejercicio publicitario en ordenamientos jurídicos como el europeo es importante para entender cuál es la tendencia y el posible desarrollo con la normativa que ha entrado a regir en Colombia.

3.1.1 Reglamento No. 45/2001 Del Parlamento Europeo y del Consejo de 18 de diciembre de 2000

El parlamento Europeo y el consejo de la Unión Europea tenían como objetivo principal la creación de un sistema completo de protección de datos personales, en el cual no solo se requería únicamente establecer los derechos de las personas cuyos datos se tratan y las obligaciones de quienes tratan dichos datos personales, sino también unas sanciones apropiadas para los infractores y un organismo supervisor independiente. Este reglamento comenzó a regir en Europa a partir del 18 de diciembre del año 2001.

[35] IBID, p.19.

De este reglamento creado en diciembre del año 2000 cabe destacar que existe gran similitud con el derecho Colombiano. Entre los puntos que han tratado en este reglamento es importante mencionar el tratamiento que se le da a la transmisión de datos personales a destinatarios distintos de las instituciones y los organismos comunitarios y no sujetos a la Directiva.

> Los datos personales sólo se podrán transmitir a destinatarios distintos de las instituciones y los organismos comunitarios y no sujetos al Derecho nacional adoptado en aplicación de la Directiva 95/46/CE cuando se garantice un nivel de protección suficiente en el país del destinatario o en la organización internacional destinataria, y los datos se transmiten exclusivamente para permitir el ejercicio de las tareas que son competencia del responsable del tratamiento.
>
> …
>
> La suficiencia del nivel de protección ofrecido por el tercer país o la organización internacional de que se trate se determinará a la luz de todas las circunstancias que rodean la operación de transmisión de datos o el conjunto de operaciones de transmisión de datos. Se tendrá particularmente en cuenta la naturaleza de los datos, la finalidad y la duración de las operaciones de tratamiento propuestas, el tercer país o la organización internacional de destino final, los preceptos legales generales y sectoriales vigentes en el tercer país o aplicables a la organización internacional de que se trate, así como las normas

> profesionales y las medidas de seguridad observadas en ese país u organización internacional.[36]

Lo anterior, es importante porque hace referencia a una situación que se encuentra en un momento circunstancial del derecho internacional. El 6 de octubre de 2015 el Tribunal Europeo de Justicia decidido anular el acuerdo de Puerto Seguro que permitía a compañías transferir datos desde Europa a Estados Unidos al considerar que éstos no están lo suficientemente protegidos en el país norteamericano. La razón por la cual el tribunal europeo de justicia considera que Estados Unidos no es considerado un lugar seguro para el tratamiento de datos tiene su origen en las demandas presentadas por Maximillian Schrems. Un ciudadano austríaco de 27 años, doctor en derecho, que había presentado varias demandas contra Facebook y otras empresas tecnológicas al considerar que al transferir sus datos a Estados Unidos violaban su derecho a la privacidad. La sentencia y la demanda, deben entenderse como una de las consecuencias del caso Snowden en el año 2013, en las que desvelaba los programas de espionaje masivos por parte del gobierno de Estados Unidos sobre los datos almacenados por todas las empresas tecnológicas.

La norma colombiana determina que la entidad encargada para definir qué se considera como una lugar o Estado seguro o inseguro para el tratamiento de datos personales es la Superintendencia de Industria y Comercio, razón por la cual debe esperarse el concepto de la misma. Sin embargo, es necesario tener en cuenta que independientemente del concepto que emita la Superintendencia con respecto a los

[36] EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,. (2001). *REGLAMENTO (CE) No 45/2001 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 18 de diciembre de 2000*. Bruselas: Diario Oficial de las Comunidades Europeas.

Estados Unidos, sería descontextualizado pensar que la Superintendencia no va a tener en cuenta las consideraciones realizadas por el Tribunal de Justicia Europeo con respecto a la seguridad proporcionada por los Estados Unidos.

3.1.2 DIRECTIVA 2009/136/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 25 DE NOVIEMBRE DE 2009

El objeto del Parlamento Europeo al emitir esta directiva fue precisamente el de establecer los derechos de los usuarios finales y las correspondientes obligaciones de las empresas que proporcionan redes y servicios de comunicaciones electrónicas disponibles al público.

Adicionalmente, se puede identificar dentro de la norma unas disposiciones enfocadas específicamente en el tema que se está abordando en este proyecto. La pregunta que se hace en este trabajo con respecto a cuáles son los límites al tratamiento de información de datos personales en el marco de la publicidad y el mercadeo, se puede encontrar en gran medida la respuesta dada por los órganos competentes europeos en el artículo 13 de esta directriz.

1. La utilización de sistemas de llamada automática y comunicación sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa solo se podrá autorizar

respecto de aquellos abonados o usuarios que hayan dado su consentimiento previo.

2. No obstante lo dispuesto en el apartado 1, cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de la venta de un producto o de un servicio de conformidad con la Directiva 95/46/CE, esa misma persona física o jurídica podrá utilizar dichas señas electrónicas para la venta directa de sus propios productos o servicios de características similares, a condición de que se ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan y, en caso de que el cliente no haya rechazado inicialmente su utilización, cada vez que reciban un mensaje ulterior.

3. Los Estados miembros tomarán las medidas adecuadas para garantizar que no se permitan las comunicaciones no solicitadas con fines de venta directa en casos que no sean los mencionados en los apartados 1 y 2, bien sin el consentimiento del abonado o el usuario, bien respecto de los abonados o los usuarios que no deseen recibir dichas comunicaciones. La elección entre estas dos posibilidades será determinada por la legislación nacional, teniendo en cuenta que ambas opciones deben ser gratuitas para el abonado o usuario.

4. Se prohibirá, en cualquier caso, la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación, o que contravengan lo dispuesto en el artículo 6 de la Directiva 2000/31/CE, o que no contengan una dirección válida a la que el destinatario pueda enviar una petición de que se ponga fin a tales comunicaciones o en los que se aliente a los destinatarios a visitar páginas web que contravengan el artículo 6 de la Directiva 2000/31/CE[37]

De forma complementaria es importante señalar y destacar las políticas de la Unión Europea con respecto al uso de cookies. En la misma directriz, en el punto 66 se establece lo siguiente sobre las cookies.

> Puede que haya terceros que deseen almacenar información sobre el equipo de un usuario o acceder a información ya almacenada, con distintos fines, que van desde los fines legítimos (como algunos tipos de cookies) hasta aquellos que suponen una intrusión injustificada en la esfera privada (como los programas espía o los virus). Resulta, por tanto, capital que los usuarios reciban una información clara y completa cuando realicen una acción que pueda dar lugar a dicho almacenamiento u obtención de acceso. El modo en que se facilite la información y se ofrezca el derecho de negativa debe ser el más

[37] EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,. (2009). *DIRECTIVA (CE) No 136/2009 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 25 de noviembre de 2009*. Bruselas: Diario Oficial de las Comunidades Europeas.

> sencillo posible para el usuario. Cuando sea técnicamente posible y eficaz, de conformidad con las disposiciones pertinentes de la Directiva 95/46/CE, el consentimiento del usuario para aceptar el tratamiento de los datos puede facilitarse mediante el uso de los parámetros adecuados del navegador o de otra aplicación.[38]

Lo anterior, supone tener un conocimiento básico de que es una "cookie". Una cookie, complementando los anteriormente expuesto, es un archivo de almacenamiento de información en formato de texto que los sitios web instalan en el computador o el dispositivo móvil de los usuarios que los visitan. Las cookies hacen posible que el sitio web recuerde las acciones y preferencias del usuario.

Continuando con la línea base creada por el parlamento europeo, de cuáles son los límites al uso de información y datos personales de las personas cuando existen fines comerciales de mercadeo y publicidad, cabe anotar, que el numeral 67 de la directriz hace referencia a las garantías ofrecidas a los individuos mediante comunicaciones no solicitadas con fines de venta directa mediante SMS[39], MMS[40] y otros tipos de

[38] EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA. (2009). *DIRECTIVA (CE) No 136/2009 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 25 de noviembre de 2009*. Bruselas: Diario Oficial de las Comunidades Europeas.

[39] **SMS**: servicio de mensajes cortos o servicio de mensajes simples, más conocido como SMS (por las siglas del inglés *Short Message Service*), es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos, conocidos como mensajes de texto, entre teléfonos inteligentes. .Disponible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:es:PDF . Tomado el 1 de febrero de 2016.

[40] **MMS**: El servicio de mensajería multimedia o MMS (siglas del término en inglés *Multimedia Messaging Service*) es un estándar de mensajería que le permite a los teléfonos móviles enviar y recibir contenidos multimedia, incorporando sonido, video o fotos.[1] La mensajería multimedia permite el envío de estos contenidos además a cuentas de correo electrónico, ampliando las posibilidades de la comunicación móvil, pudiendo publicar fotografías digitales o actuar en weblogs sin la mediación de una computadora. Disponible en http://eur-

aplicaciones similares debido a que a estos deben ser aplicables las mismas políticas que a correos electrónicos.

Sobre el panorama Europeo se puede decir que a grandes rasgos se crean unos canales regulados de conectividad entre el oferente del producto o servicio que está aplicando estrategias comerciales y el usuario persona natural o empresa que es el consumidor final del cual se están tratando datos personales. Independientemente de la tecnología que se esté utilizando, SMS (mensaje de texto), correo electrónico, mensaje por whatsapp, llamada telefónica, inserción de cookies en el navegador, existen tres elementos básicos que están presentes en cualquier situación de contacto.

El primer elemento, es la autorización. Si el usuario, persona natural, considera que no dio la autorización o que quiere revocar la autorización para que lo contacten, deben existir formas previstas por el encargado de tratar las bases de datos para dar de baja o al menos dar el instructivo para dejar de contactar a aquella persona.

El segundo elemento, es la identidad clara y expresa de la empresa, persona jurídica, corporación u organización que está contactando al usuario persona natural objeto de las actividades comerciales. En ningún momento se puede ocultar la identidad del encargado del tratamiento de los datos personales.

El tercer elemento, que se encuentra como una constante y elemento fundamental en el ejercicio de datos personales para fines comerciales es la usabilidad de la plataforma para realizar las acciones por medios de las cuales se ejercen los derechos de habeas

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:es:PDF. Tomado el 1 de febrero de 2016.

data. En otras palabras, la directriz es clara en exigir que la forma por medio de la cual los usuarios pueden conocer la información que de ellos se tenga, actualizarla, modificarla o eliminarla, debe ser la más sencilla posible. En efecto, muchas plataformas o páginas web, le notifican inmediatamente a un usuario que ingresa al sitio web, que ese mismo utiliza cookies para almacenar información de navegación.

3.2 ESTADOS UNIDOS

Estados Unidos es uno de los países más controversiales en este tema por las formas y los usos que le ha dado históricamente a las bases de datos personales y todo lo que tiene que ver con la forma de cómo un gobierno y la industria interviene en la privacidad y controla la información de su población. Es uno de los países en el mundo con mayor grado de intervención en la información de las personas, violando los derechos de intimidad y privacidad. Todas estas circunstancias, entre otras, reflejan la ausencia de una ley federal en los Estados Unidos de América que proteja de manera amplia y completa todo el tratamiento de datos, porque si bien es cierto que existen múltiples leyes relacionadas con el tema, se basan en actividades específicas, o tipos de información, o agentes determinados. Es por esto que aún se necesita una ley federal que regule la recolección de las bases de datos y el uso que se le da a ella, en una forma clara y detallada. Este es uno de los factores por los cuales se hizo necesario realizar un tratado bilateral con Europa, Tratado de Puerto Seguro, el cual ya fue explicado.

Entrando en detalle, el sistema de normas que utiliza este país, muchas veces, hace muy confusa la materia a juzgar por las contradicciones, vacíos, extralimitaciones pues

finalmente funciona como un montón de normas que deberían encajar perfectamente tanto a nivel federal como a nivel estatal, pero en la realidad no sucede así. Entonces, en un primer momento no se cuenta con una ley federal que hable del tema de manera clara y extensa y, en segundo lugar, se encuentran un gran número de guías y marcos elaboradas por agencias del gobierno y grupos privados que, aunque no tienen fuerza de ley funcionan como marcos y guías de autorregulación las cuales son denominadas "buenas prácticas".[41] Algunos ejemplos de leyes existentes relacionadas con el tema son:

1. The Children's Online Privacy Protection Act (COPPA)
2. S. 1158 (Consumer Privacy Protection Act)
3. H.R. 2092 (Student Digital Privacy and Parental Rights Act)
4. S. 668 (Data Broker Accountability and Transparency Act)
5. The Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act) es una ley federal sobre la protección del consumidor que prohíbe prácticas injustas o engañosas la cual es aplicada a prácticas en línea como fuera de linea y políticas de seguridad de datos.
6. The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)) (15 U.S.C. §§6801-6827) esta ley regula a todas las entidades que presten servicios financieros y como estas realizan la recolección, uso y revelación de datos personales

[41] Partner, I. (2015). *Practical Law*. *Us.practicallaw.com*., Disponible en http://us.practicallaw.com/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1248063181319&ssbinary=true Tomado el 15 febrero de 2016.

7. The Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.) esta regula todas las entidades que tengan contacto con información médica, desde farmacias hasta hospitales.

A nivel estatal, la mayoría de los Estados, cuentan con leyes de privacidad, pero el Estado de California se ha destacado por su avanzada en el manejo de datos personales y privacidad. En este Estado se han sancionado múltiples leyes en este tema, muchas de las cuales han tenido un alcance nacional en la práctica. Además, de que estas leyes siguen el modelo de regulación Europeo, teniendo en cuenta que este último es mucho más estricto y proteccionista a favor de las personas. Por ejemplo, uno de las leyes ejemplares en california, The Shine the Light law, la cual ahora hace parte del código civil de california, obliga a las compañías a destapar al público con cuales terceros comparten la información personal y con qué fines, además, que deben brindar mecanismos eficientes que permitan a las personas elegir si desean que su información personal sea transferida a terceros. Por otro lado, se debe indicar si estos terceros utilizan dicha información con fines comerciales. Por último, obliga a las compañías a establecer protocolos de seguridad para que esta estas bases de datos no sean accedidas por usuarios no autorizados, para evitar su destrucción, mal uso, modificación o publicación. Un fragmento de esta ley dice así, *1798.81*.

> Una empresa tomará todas las medidas razonables para disponer, o hacer que se ocupen de la eliminación, de los registros de clientes dentro de su custodia o control que contiene información personal cuando los registros no se vayan a guardar por más tiempo por el negocio por medio de (a) la trituración, (b) el borrado, o (c) modificar

de otro modo la información personal en esos registros para que sea ilegible o indescifrable a través de cualquier medio.

Otra cara de la moneda en cuanto a la regulación en los Estados Unidos y el tema visto tiene que ver con la autoridad competente para sancionar los incumplimientos de las prácticas realizadas por fuera de los parámetros, tanto legales como sociales. Se dice que la FTC (Federal Trade Commission) la Comisión Federal de Comercio es el principal actor en la sanción y la vigilancia de este tipo de normas. Si bien es cierto que otras agencias como las bancarias pueden hacer cumplir las normas, las facultades que tiene la Comisión Federal de Comercio son mucho más amplias y contundentes. Estas van desde la iniciación de una investigación hasta desistir de ella, pero también podrá interponer quejas ante una Corte. Ahora, teniendo en cuenta lo anterior, recordando que la Comisión es el agente más activo dentro del territorio americano este actor no puede ni vigilar ni sancionar a todos los infractores, pues su jurisdicción, en cuanto a los sujetos es limitada. Existen agremiaciones las cuales tienen agencias gubernamentales controlándolas, pero de manera independiente. Por ejemplo, transporte, telecomunicaciones y el sector financiero. En consecuencia, la Comisión Federal de Comercio se limita a las compañías y personas que realizan negocios dentro de los Estados Unidos, y, además, a las páginas web que estén utilizando publicidad comportamental.[42]

3.3 TERRITORIALIDAD DE LA LEY

[42] Ibid. Pg 3

Esta es una problemática que cobra importancia en la medida que las plataformas digitales, las páginas web, las aplicaciones y todos los servicios en línea van adquiriendo vocación global y por ende cabe mirar que sucede cuando una persona, residente en un país accede a una página en la que se recopilan sus datos y son usados por una empresa extranjera cuya presencia en el país de residencia del titular de los datos solo es vía la página web, sin necesidad de que tengan una oficina abierta en el mismo. Si bien en otras secciones de esta tesis se ha hecho referencia a empresas como Facebook, Google, Youtube para dar ejemplo de multinacionales que ejercen actividades de minería de datos, es importante tener en cuenta que estas como su nombre lo indica son multinacionales y por ende tienen sede en la mayoría de los países del mundo.

La pregunta aquí, es entender que sucede con empresas como Godaddy, Wetransfer, Amazon, Vimeo, entre otras. Todas estas empresas tienen en común, que son utilizadas frecuentemente por personas de todo el mundo, y sin embargo la gran mayoría de ellas no abarca, territorialmente hablando, más de 2 máximo 3 países en los cuales tienen sedes. Estas empresas recolectan datos como los correos electrónicos, información de tarjetas de crédito, direcciones de entrega y hábitos de consumo de video. ¿Cómo trata este tema el derecho comprado?

Para efectos de entender y de dar respuesta a la pregunta aquí planteada, cabe mirar un caso puntual en donde se presenta exactamente este supuesto jurídico y al cual el Tribunal de Justicia Europeo tuvo que dar respuesta mediante sentencia que constituye

precedente jurisprudencial. A continuación, se va a exponer el caso de manera resumida tomado directamente de la página del Tribunal de Justicia Europeo ¨Info Curia¨ [43]

Weltimmo, sociedad constituida en Eslovaquia, gestiona un sitio de Internet de anuncios de inmuebles situados en Hungría. Los anuncios son gratuitos durante un mes, trascurrido el mes, el servicio pasa a ser pago. Varios anunciantes solicitaron por correo electrónico, la retirada de sus anuncios a partir del cumplimiento del mes, así como la supresión de sus datos personales. Sin embargo, Weltimmo no los suprimió y facturó sus servicios a los anunciantes. Debido al no pago de las facturas, Weltimmo transmitió los datos de los anunciantes a empresas de cobro.

Los anunciantes presentaron denuncias ante la autoridad húngara de control. Ésta se declaró competente, por considerar que la recogida de los datos había tenido lugar en el territorio húngaro y que constituía un tratamiento o un procesamiento de datos relativos a unas personas. Dicha autoridad de control consideró que Weltimmo había infringido la Ley sobre la información e impuso a la citada sociedad una multa de alrededor de 32 000 euros.

Weltimmo recurrió en casación ante el Tribunal de Justicia Europeo alegando que en virtud del artículo 4, apartado 1, letra a), de la Directiva 95/46, la autoridad húngara de control, en el presente caso, carecía de competencia y no podía aplicar el Derecho húngaro a un prestador de servicios establecido en otro Estado miembro. Weltimmo sostuvo que, con arreglo al artículo 28, apartado 6, de la Directiva 95/46, dicha

43 http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=182564

autoridad debió haber instado a la autoridad eslovaca competente en la materia a que actuara en su lugar.

A continuación se cita el texto de la decisión tomada por el Tribunal de Justicia Europeo…

> El artículo 4, apartado 1, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que permite aplicar la legislación relativa a la protección de los datos personales de un Estado miembro distinto de aquel en el que está registrado el responsable del tratamiento de esos datos, siempre que éste ejerza, mediante una instalación estable en el territorio de dicho Estado miembro, una actividad efectiva y real, aun mínima, en cuyo marco se realice el referido tratamiento.
>
> Para determinar si así ocurre, en circunstancias como las controvertidas en el litigio principal, el órgano jurisdiccional remitente puede tener en cuenta, por un lado, que la actividad del responsable de dicho tratamiento, en cuyo marco éste tiene lugar, consiste en la gestión de sitios de Internet de anuncios de inmuebles situados en el territorio de dicho Estado miembro y redactados en la lengua de ese Estado y que, en consecuencia, se dirige principalmente, incluso íntegramente, a dicho Estado miembro y, por otro lado, que ese responsable dispone de un representante en el referido Estado miembro que se encarga de

> cobrar los créditos resultantes de dicha actividad y de representarlo en los procedimientos administrativo y judicial relativos al tratamiento de los datos en cuestión.

Ahora bien, el caso anterior expone algunas luces sobre la materia y con respecto a manejo y las decisiones adoptadas por la Unión Europea, sin embargo no se puede dejar de lado otra herramienta internacional que cumple el mismo propósito de armonizar las situaciones de territorialidad. El instrumento al que se hace referencia es el marco sobre privacidad de la OCDE.[44] Documento expedido originalmente en 1980 y actualizado en el año 2013 establece una serie de principios en materia de privacidad y de datos personales, como recomendaciones para que todos los países miembros las sigan.

En la parte cuatro del marco de políticas de privacidad de la OCDE o como aparece publicado ¨ THE OECD PRIVACY FRAMEWORK¨ se aborda el tema de flujo transfronterizo de datos personales, las restricciones legítimas y los principios básicos de aplicación internacional. La siguiente es una traducción de estos artículos.
16. El responsable del tratamiento de los datos, es responsable de los datos bajo su custodia, independiente a la ubicación de los datos. 17 Un país miembro debe de abstenerse de restringir el flujo de datos personales entre su país y otros países miembros, siempre y cuando el otro país garantice efectivamente el cuidado y tenga medidas coercitivas y apropiadas para la protección de los datos personales de las personas de forma continua. 18. Cualquier restricción transfronteriza en el flujo de datos personales debe estar justificada en el riesgo medido, teniendo en cuenta la sensibilidad del dato, y el propósito o la finalidad de su procesamiento. 20. Los países miembros deben adoptar medida que faciliten la aplicación legal transfronteriza

[44] http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

cooperativa. 21. Los países miembros deben apoyar y promover el desarrollo de tratados o acuerdos internacionales en donde surjan efectos prácticos de los lineamientos aquí planteados.

4 POLÍTICAS DE GOOGLE EN TRATAMIENTO DE DATOS PERSONALES Y PUBLICIDAD

Si bien hablar de Google es tocar el caso de una empresa en particular, es indiscutible que esta empresa es la más relevante e importante en el panorama actual. Calificada como la empresa con más tráfico a nivel mundial y dueña de YouTube, plataforma que también está en el ranking de las 5 páginas más visitadas en Colombia y a nivel mundial, adicionando el hecho que es la empresa de publicidad más grande del mundo y que realiza constantemente actividades de big data[45], se presenta como un caso de observación necesario para el objetivo de esta estudio.

[45] El Big Data o Datos masivos es un concepto que hace referencia a la acumulación de grandes cantidades de datos y a los procedimientos usados para encontrar patrones repetitivos dentro de esos datos.

Cuando un usuario crea una cuenta en Google, ya sea para obtener una cuenta de correo electrónico, o para utilizar cualquiera de los servicios que ofrece como drive, docs, sheets, youtube, entre otros, entrega una serie de datos personales a esta empresa. Datos como su nombre, fecha de cumpleaños, edad, numero de celular. La empresa siempre consulta al usuario si acepta los términos y condiciones del servicio, entre estos términos y condiciones se encuentran las políticas de uso y tratamiento de los datos personales.

Las políticas responden a unas preguntas básicas, estas son; qué datos recoge, con qué fines, cómo utilizan los datos, cómo pueden las personas acceder a los datos y actualizarlos. En el primer caso la empresa se da a la tarea de describir las clasificaciones de los tipos de datos que se recolectan. En primer lugar, se puede identificar los datos proporcionados directamente por el usuario como el nombre, correo electrónico, celular, número de tarjeta de crédito.

En segundo lugar, están los datos obtenidos por el uso de los servicios de Google. Estos tienen unas subcategorías, la primera es la información del dispositivo, en ese caso Google recopila información específica del tipo de dispositivo como el modelo y el hardware, la versión del sistema operativo, información de la red de telefonía móvil y el número de teléfono. La segunda categoría son los datos de registro, esto consiste en almacenar toda la información de navegación del usuario al guardar las consultas hechas en el buscador, el contenido propio de Google consultado. La ubicación física es el tercer elemento al que hace alusión. En palabras textuales de Google;

> Cuando utilizas los servicios de Google, podemos recopilar y procesar información sobre tu ubicación real. Empleamos diferentes tecnologías para determinar la ubicación, como la identificación de la dirección IP[46], el sistema GPS y el uso de otros sensores que pueden proporcionar a Google, por ejemplo, información sobre dispositivos cercanos, puntos de acceso Wi-Fi y antenas de telefonía móvil.[47]

Por último, hacen mención al uso de cookies para almacenar información de navegación de cada uno de los usuarios. La empresa hace la aclaración que solo le da tratamiento de datos personales a estas empresas a partir del momento que asocia la información de navegación con el usuario de Google, y por tanto solo les da tratamiento de datos personales a esa información a partir del momento que esté identificada la persona.

Atendiendo a la segunda pregunta que hace referencia al con que fines son utilizados estos datos, vale la pena mirar los siguientes apartados del texto original de las políticas de la empresa.

> Utilizamos la información que recogemos de todos nuestros servicios para proporcionarlos, mantenerlos, protegerlos y mejorarlos, para desarrollar otros nuevos y para proteger a Google y a nuestros usuarios.

---

[46] IP: Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz en red (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del modelo OSI. Disponible en http://www.mon-ip.com/es/mi-ip/ . Tomado el 15 de febrero de 2016.

[47] Google.com,. (2016). *Política de Privacidad – Privacidad y condiciones – Google.*, Disponible en https://www.Google.com/intl/es-419/policies/privacy/ o https://static.Googleusercontent.com/media/www.Google.com/es//intl/es-419/policies/privacy/Google_privacy_policy_es-419.pdf Tomado de 15 febrero 2016

> También utilizamos estos datos para ofrecerte contenido personalizado como, por ejemplo, resultados de búsqueda y anuncios más relevantes.
> …
> Utilizamos la información que recogemos de cookies y otras tecnologías, como las etiquetas, para mejorar tu experiencia de usuario y la calidad general de nuestros servicios. Uno de los productos que utilizamos para llevar a cabo esta actividad con nuestros propios servicios es Google Analytics. Por ejemplo, al guardar tus preferencias de idioma, podremos mostrar nuestros servicios en el idioma que prefieras. Al mostrarte anuncios personalizados, no asociaremos identificadores de cookies ni de ninguna tecnología similar a categorías sensibles de datos como, por ejemplo, las que hacen referencia a la raza, a la religión, a la orientación sexual o a la salud.[48]

En repetidas ocasiones se refieren a los anuncios, los cuales son personalizados o que son más relevantes para la experiencia de navegación del usuario. Esto se podría describir como el punto en donde se conecta toda la problemática que aborda esta monografía, la información y el uso de datos personales con fines publicitarios.

Es así como una empresa con la experiencia que tiene Google, hace un uso óptimo de los datos personales de sus usuarios para publicarles ofertas de los anunciantes. De esta misma manera empresas como Twitter, LinkedIn, Facebook, además de Google, han creado una industria que mueve billones de dólares cada año a nivel mundial con lo que los expertos en medios y publicidad llaman compra programática de audiencias.

[48]Ibid. Pg 10

Juzgar si la práctica es positiva o negativa no es el objetivo de esta monografía, aquí la finalidad es meramente descriptiva del fenómeno que se vive en la actualidad.

La última de las preguntas a la cual le da respuesta las políticas de privacidad de Google es, como pueden las personas conocer y actualizar los datos que de ellos se tengan. Esta empresa ha creado un servicio de acceso a la información personal. Por este medio las personas pueden, ingresando con su correo electrónico a un servicio web, conocer actualizar y eliminar algunos de los datos que de ellos se tengan. Es importante resaltar que el acceso para los datos personales es de forma gratuita, sin embargo, estas empresas evaden la responsabilidad al establecer como límite, el hecho que si el usuario está solicitando una acción que obligue a la empresa a realizar unas actividades desproporcionadas o desarrollos adicionales, Google no se verá obligado al cumplimiento.

5 MODELOS DE PUBLICIDAD DIGITAL

La publicidad digital entra en el marco de lo que se puede clasificar como el marketing digital o cyber-marketing. Hablar de marketing digital es abordar un universo de estrategias, herramientas y aplicaciones que abarcan muchos más campos que el que se pretende abordar en este estudio, “el tratamiento de datos personales para la aplicación de estrategias publicitarias”.

En este capítulo vamos a hacer una exposición general que permita al lector no experto, tener un contexto de lo que es el marketing digital. Luego se hará énfasis en los modelos de publicidad digital, explicando cómo funcionan y qué relación tienen con el tratamiento de datos personales por parte de aquellos anunciantes que administran bases de datos con información de sus clientes y el público en general.

Por definición y en un sentido práctico la diferencia entre marketing y publicidad se puede ver de la siguiente manera; mientras que el mercadeo es el ejercicio que hace aquel encargado de desarrollar todas las estrategias posibles para lograr que un producto o servicio sea adquirido por un consumidor objetivo, la publicidad es aquella tarea desempeñada para que la empresa dé a conocer la marca, producto o servicio a una audiencia determinada.

Puede que a primera vista no sea evidente la diferencia, pero con el siguiente ejemplo se entenderá de forma más clara la diferencia entre mercadeo y publicidad. Un diseñador de ropa que vende vestidos de lujo a un alto costo tiene claro que su estrategia de mercadeo es no hacer publicidad, debido a que parte del valor agregado que ofrece a sus pocos clientes es la exclusividad en sus vestuarios. En el anterior ejemplo se puede ver como una estrategia de mercadeo puede basarse netamente en limitar la oferta para incrementar el precio y por ende no requiere de publicidad, mientras que en la publicidad el objetivo siempre es, como su nombre lo indica, publicar la oferta, sin importar qué tan limitada esta sea.

El mundo del mercadeo en plataformas digitales tiene muchas capas. Siendo un mundo relativamente nuevo en el cual no todos los usuarios son expertos y teniendo en cuenta que está constantemente evolucionando, no es posible decir que hay unos conceptos unificados para clasificar los distintos momentos de contacto que se viven en el mundo del mercadeo digital, sin embargo, existen muchas empresas que lo desglosan en las siguientes etapas.

Primera, contactar la audiencia; segunda, capturar la audiencia; tercera, fidelizar los usuarios; cuarta, convertir o monetizar los usuarios; por último, expandir el consumo

de sus usuarios. Los productos y servicios que se están ofreciendo pueden ser físicos, como un par de zapatos o pueden ser digitales, como pagar una suscripción en una plataforma de contenido en demanda. El medio digital puede servir como una plataforma transaccional, por ejemplo, cuando el usuario paga con su tarjeta de crédito en la página web del que está ofreciendo los zapatos, o puede operar como plataforma de contacto, caso en el cual solicita él envió de los zapatos y los paga contra entrega en su hogar.

Si el usuario que realizó la compra tuvo una buena experiencia, lo más seguro es que vuelve a comprarle al oferente. En términos de las fases del mercadeo digital esta sería la fase de expansión. El momento de conversión o monetización se da cuando el usuario realizó esa compra, y ese momento es producto del proceso de fidelización en el cual le estuvieron mostrando durante un tiempo una variedad de cosas como; una amplia gama de zapatos hasta llegar a los que él quería, información de que la pagina es segura, descuentos en diferentes artículos, posibilidades de ganar premios por compras en la página, entre otras estrategias de fidelización y conversión.

Con respecto a los otros dos momentos a los que se hace mención, contactar y captar la audiencia, cabe aclarar que son los momentos dentro de las estrategias de mercadeo digital en los cuales la publicidad y los datos personales juegan el rol más importante. Es en el momento en el que al usuario sentado en su computador le está apareciendo el banner ofertando unos zapatos. La publicidad debe estar bien dirigida, y bien invertida, de modo que logre capturar a ese usuario navegando en línea, debe lograr que el usuario le dé clic al banner con la oferta y comenzar a navegar en el portal de la marca de zapatos. Es ahí, en este punto, en donde se va a concentrar el resto de este capítulo, explicando los distintos modelos de publicidad digital y entre otros ejemplos, explicar

cómo es posible que el anunciante tuviera suficiente información del sujeto como para saber que es un hombre de 45 años que está buscando zapatos nuevos.

A continuación, se hará una descripción de algunos tipos de publicidad en medios digitales. El primer caso a exponer es el mailing o publicidad por medio del correo electrónico. Los correos electrónicos directos son el comienzo de la publicidad en internet. Este modelo publicitario consiste en enviar mensajes publicitarios a través de correos electrónicos, y si bien este tipo de publicidad está desde los primeros momentos desde que la publicidad comenzó en los medios digitales y ha logrado sobrevivir hasta la fecha, cabe aclarar que ha perdido efectividad. En la medida que los usuarios adquieren mayor experiencia en el manejo de sus bandejas de entrada, son más los correos directos con contenido promocional que van directo a la bandeja de correo no deseado o correo basura. Con respecto al mailing o envío de correos electrónicos masivos es importante aclarar que estos son el punto de partida para la obtención de bases de datos de un individuo. Sobre lo anterior no sobra mencionar que el correo electrónico de uso personal o de uso corporativo, educativo etc. es el primer dato personal que están obteniendo los anunciantes.

Otra de las formas, y de hecho el formato más popular en el mercado publicitario digital, es el banner. La palabra es una adaptación de formato tradicional utilizado en televisión en el cual pasaba una imagen de tipo rectangular ocupando una parte de la pantalla en su parte inferior con el contenido promocional del anunciante. El banner digital es una forma sencilla de ubicar el anuncio, situando la imagen en la página web. Los banners pueden ser recuadros que aparecen en la página principal de la página web, en secciones determinadas, pueden aparecer en la parte superior de la página o pueden estar localizados en columnas al margen del contenido. Dependiendo de la tecnología,

la cual se ha caracterizado por la tendencia de ser responsivo[49], los banners se adaptan al dispositivo en donde se esté visitando la página web, sea móvil, Tablet o pc.

La publicidad en formato de banner no presenta grandes conflictos frente al régimen de protección de datos personales. Los anunciantes que exhiben su publicidad en un banner no están obteniendo información personal de los usuarios a los que les están llegando. El anunciante tradicional que compra publicidad en formato de banner, supóngase en un medio como el tiempo.com o minuto30.com está comprando impresiones. Una impresión es contada cada que un usuario navegando en línea, ingresa a una página web y le es exhibido el banner publicitario.

Los anunciantes obtienen tendencias, más no datos personales. A modo de ejemplo estas tendencias pueden ser caracterizadas de la siguiente manera; 100.00 impresiones, 45% hombres 55% mujeres, 35% de las vistas en Miami, 20% Paris, 15% Bogotá. Usuarios entre los 10 - 15 años 20%, 15-25 años 35%, etc.

Se puede identificar el formato de floating ad[50] cuando un usuario abre una página web y aparece un anuncio flotando en su pantalla sobre la ventana que acabo de abrir, por

[49] El diseño web adaptable, adaptativo o responsivo, conocido por las siglas RWD del inglés Responsive Web Design, es una filosofía de diseño y desarrollo cuyo objetivo es adaptar la apariencia de las páginas web al dispositivo que se esté utilizando para visualizarla. Hoy día las páginas web se visualizan en multitud de tipos de dispositivos como tabletas, teléfonos inteligentes, libros electrónicos, portátiles, PC, etcétera. Además, aún dentro de cada tipo, cada dispositivo tiene sus características concretas: tamaño de pantalla, resolución, potencia de CPU, capacidad de memoria, entre otras. Esta tecnología pretende que con un solo diseño web, se tenga una visualización adecuada en cualquier dispositivo. Disponible en http://www.mischunches.com/diseno/diseno-sitios-web-adaptables.php . Tomado el 10 de febrero de 2016.

[50] Un anuncio flotante , o anuncio de superposición , es un tipo de anuncio con animaciones que aparece superpuesta sobre el contenido de la página web solicitada . anuncios flotantes pueden desaparecer o ser menos invasivos después de un período de tiempo preestablecido. Disponible en

lo general estos anuncios suelen ser una especie de animación con la posibilidad de añadirles sonido o música. El expanding ad es el formato caracterizado por expandirse cuando el usuario navegando en la página web cursa su mouse sobre el banner que en principio tiene formato tradicional. Los Pop-ups son los formatos tradicionales que se caracterizan por abrir una página web cuando un usuario navegando en línea le da click a una página determinada. En otras palabras, este es un formato que además de abrir la página web que el usuario desea abrir, está abriendo una segunda página web en donde se encuentra contenido promocional.

Todos estos modelos de publicidad digital mencionados en el anterior párrafo son modelos considerados como intrusivos. En algunos casos estos sistemas pueden estar operando como un virus en el computador, en otros casos son formatos publicitarios reconocidos por ser malas prácticas en el medio. De por sí, estos modelos no intervienen con datos personales de los individuos, se pueden comparar al banner tradicional. En otras ocasiones estos formatos son creados exclusivamente para obtener datos personales. A modo de ejemplo se puede ver el caso de la página éxito.com. Cada que un usuario ingresa a la plataforma aparece de inmediato un pop up, en el cual le solicita a la persona que ingrese como usuario o que se registre con su correo electrónico, este es el formato tradicional de publicidad digital, utilizado para obtener el dato personal básico de contacto de las personas, su correo electrónico.

El video es uno de los formatos más populares y más respetados, tanto por los anunciantes como por los consumidores de internet. Hay algunas empresas que gastan

https://support.Google.com/adwordspolicy/answer/176108?hl=es-419 . Tomado el 10 de febrero de 2016.

millones de dólares en producciones audiovisuales que no parezcan publicidad intrusiva, sino que sean contenido entretenido en el cual haya relación directa con la marca. Un ejemplo de este caso fue la inversión hecha por la empresa Bavaria para su línea de cerveza Poker. Utilizando un medio publicitario no tradicional ni siquiera para los medios digitales, Bavaria, asesorada por la empresa Havas Media en la ciudad de Bogotá, creó una serie web para ser emitida en YouTube. La serie Entre Panas de la cerveza póker, en la cual se representan distintos momentos de interacción de un grupo de amigos con sus cervezas es un modelo publicitario basado en video.

YouTube es la plataforma más común para anunciar con video, sin embargo, empresas como RCN y Caracol, tienen tecnología de reproducción de videos en sus páginas web en las cuales venden tendencias de audiencias. Entrar a hablar de las formas como se puede anunciar con video es abordar todo un mundo sobre la publicidad en internet. Product placement[51], skip ad video[52], video fijo, banners, tarjetas y etiquetas son las principales formas para anunciar en video. En general, lo importante que se debe tener en cuenta cuando se habla de video, y con relación a este análisis, es que cuando la empresa (YouTube) logra individualizar a la persona que está viendo el video, esto si se convierte en un caso de información personal. Este es el caso de Google, dueño de YouTube, en donde pueden individualizar e identificar cuáles son los gustos y preferencias de cada consumidor de video. Entre estos gustos y preferencias se pueden

[51] Publicidad por Emplazamiento es una técnica publicitaria que consiste en la inserción de un producto, marca o mensaje dentro de la narrativa del programa (mostrado, citado o utilizado por los actores). Se utiliza por lo general en medios de comunicación audiovisual como programas y series de televisión, telenovelas, videos musicales, cine y videojuegos, entre otros. Disponible en http://www.undertv.tv/product_placement.html . Tomado el 10 de febrero de 2016.

[52] Skip ad video. La opción otorgada por la plataforma de video para que los usuarios que están visualizando los contenidos dentro de la plataforma puedan dar clic en la opción de (skip add) pasados 5 segundos a partir del momento en que el reproductor comienza a emitir un mensaje publicitario automático y salir del video del anuncio para dirigirse al contenido.

destacar datos como que un usuario determinado consume 2 horas de videos de motocross, 3 horas de vídeos de deportes extremos y 2 horas de motos de alto cilindraje, esta es suficiente información para que la empresa pueda publicitar a este usuario ofertas utilizando la información personal que de él tiene.

Luego de hablar de YouTube como el reproductor de video más importante en Colombia y el mundo, no sobra anotar de nuevo que YouTube es una de las plataformas en línea que le pertenecen a la empresa Google. En Google se pueden identificar también varios formatos publicitarios. El primer servicio publicitario que ofrece el motor de búsqueda de Google es por medio de las estrategias denominadas como SEO. (search engine optimization). En español esto quiere decir, optimización del motor de búsqueda. Optimizar el motor de búsqueda es un conjunto de actividades y acciones aplicadas a la página web, para que Google como motor de búsqueda logre relacionar las palabras claves de lo que una empresa está ofreciendo y de este modo lo logre conectar con lo que un usuario está buscando en Google. De alguna manera se puede entender que las estrategias SEO son situaciones en las que inversamente la empresa está entregando su información personal (quién es, qué hace, cómo funciona, cuánto cuesta) para que los usuarios puedan llegar con mayor facilidad.

El siguiente nivel para entender la publicidad con Google es relacionado con lo explicado anteriormente acerca de SEO. Toda empresa con una estrategia publicitaria clara en medios digitales hace un ejercicio de manera juiciosa tratando de optimizar su motor de búsqueda, sin embargo, si quiere garantizar que cuando un usuario esté buscando una información determinada, lo primero que vea sea el portal de su compañía, esta empresa debe invertir en un producto que ofrece Google, el cual es denominado ad words. Ad words funciona de la misma forma que funciona la

optimización del motor de búsqueda, sin embargo, en estos casos la plataforma garantiza que el anunciante pagando por esa publicidad va a ser el primero en aparecerle a los navegantes que están escribiendo las palabras claves.

En el caso explicado anteriormente se pueden identificar dos momentos relevantes. En primer lugar, es de destacar que en los motores de búsqueda no solo las empresas, sino las personas, pueden publicar información propia, a la cual el mundo entero tendrá acceso. A modo de ejemplo es interesante hacer el ejercicio de escribir el nombre de algún conocido o el nombre propio para identificar cómo en la red están exhibidos en algunas ocasiones los datos personales tanto de personas como empresas. El segundo punto importante para anotar es que, al escribir preguntas, nombre, palabras, información y textos en motores de búsqueda, se está entregando información personal. Si el usuario escribe tiquetes Miami y luego se sale del navegador, después de dos horas ingresa y se encuentra con una promoción de tiquetes para Miami, no es casualidad. Este punto se relaciona directamente al tema anteriormente explicado, sobre las cookies en los navegadores y como todo esta es información personal.

Cuando de información personal se trata, las redes sociales son las plataformas número uno para la recolección de la misma. Facebook, LinkedIn, Twitter, YouTube, Instagram, Tumblr, Google Plus son solo algunas de las principales redes sociales que se utilizan actualmente. Lo que hace característico a las redes sociales es que los generadores de contenido son los mismos usuarios de ellas, a diferencia de los medios de comunicación tradicionales en donde el generador de contenido es exclusivamente el medio, las redes sociales tienen millones de creadores de contenido.

Cada red tiene distintas características y particularidades, pero en esencia el objetivo es el mismo; es un espacio para que los usuarios puedan publicar un contenido que les permita conectarse con más usuarios en la misma red que se identifican por la afinidad que existe en algún punto o tema en específico.

En las redes sociales lo más común es que los usuarios publican asuntos de su vida cotidiana. Donde van de paseo, fotos con sus amigos, donde salen a comer, su opinión acerca de un tema de interés general, empleado o desempleado, que estudia, donde estudia, títulos o diplomas. Adicionalmente, las personas siguen temas que les interesan y pueden interactuar con el contenido que más les gusta. Esto permite identificar si siguen equipos de fútbol o jugadores de tenis. Si les gustan los carros Ford o los carros jeep, si les gusta la cocina o prefieren comida rápida.

En algunas redes sociales se ha llegado a un nivel superior en cuanto al manejo de datos personales, redes sociales como Facebook se encuentran en capacidad de identificar lo que en la ley 1581 se clasifica como datos personales sensibles, estos son la información biométrica. Hoy en día la plataforma de Facebook tiene la capacidad de identificar con los datos biométricos, quienes son las personas que aparecen en la foto que se ha publicado en la red. Otras redes como Linked in, saben si un usuario está buscando empleo, si se acabó de graduar, si le interesa el derecho o la economía, nombre de los compañeros de trabajo entre otros asuntos.

La fuente de ingreso principal de las redes sociales es la publicidad, algunas redes sociales están pasando al modelo de suscripciones pagas para eliminar la publicidad a sus usuarios, este es el caso de YouTube red. El asunto con la publicidad, los datos personales y las redes sociales, es que estas plataformas tienen acceso a una cantidad

de información personal de las personas de la cual ni el mismo Estado tiene acceso. En este orden de ideas, no son los anunciantes los que están obteniendo la información, sino que son las plataformas digitales, casi todas con domicilio en Estados Unidos.

Lo interesante es que, siendo una legislación relativamente reciente, ninguna de estas plataformas se encuentra en cumplimiento de la ley 1581 de 2012 y pasará mucho tiempo antes de que la cumplan, pero a pesar de estar fuera de la ley, para los usuarios de las redes, estas se han convertido en herramientas necesarias para la interacción diaria.

En ocasiones anteriores se ha hecho mención de las cookies. Las cookies son pequeños archivos de texto que se almacenan en el directorio navegación del computador. Las cookies se crean para hacer un seguimiento de los movimientos por el sitio web. Estas llevan un historial de la información que el usuario ha ingresado al sitio web, así como por ejemplo en una página de destinos turísticos el usuario ingrese la palabra Cancún, lo más probable es que en las barras laterales donde se publican las ofertas, todas las ofertas publicadas sean de hoteles en Cancún.

Las cookies son la herramienta por excelencia de recolección de datos sin previa autorización. La diferencia radica en que cuando un usuario se suscribe a cualquier página y comienza a navegar con un usuario determinado, es posible para los administradores de aquella página web saber todo lo que visitan y ven. En cambio, si la persona no se ha suscrito como usuario a la plataforma, la principal herramienta que tiene el administrador del navegador para saber lo que hace este usuario es una cookie. Sabiendo que en esencia una cookie es un sistema de almacenamiento de información, identificar el límite en el cual el administrador de la plataforma está violando la

privacidad del usuario, es cuestión de conocer qué tanta información está recolectando. En capítulo anterior se hizo una exposición respecto a que esta problemática ya fue abordada por la Unión Europea, caso en el cual obligan a las empresas a notificar a los usuarios de internet que un sitio web en específico utiliza cookies y con qué fines las utiliza. En Colombia por su parte, no existe expresamente, ningún tipo de disposición por parte de órganos estatales hasta la fecha.

6. FUTURO PROYECCIÓN DEL MERCADO Y LEGISLACIÓN

La importancia de este capítulo radica en la problemática planteada en las primeras líneas de este proyecto, la evolución tecnológica vive retando constantemente al derecho a mantenerse vigente. La forma como las personas y las empresas están publicitando sus marcas, productos y servicios viven en una permanente evolución, sin embargo, es claro que para lograr mayor efectividad en sus ventas los datos personales y la información de gustos y preferencias es bastante útil.

La tarea de anticipar cuál puede ser el modelo normativo aplicado al uso de datos personales para la aplicación de estrategias publicitarias es una tarea que al mismo tiempo se torna fácil y difícil. Es fácil debido a que Colombia no es el primer Estado que aborda esta problemática y eventualmente terminará adaptando normas de

ordenamientos jurídicos como el Europeo, en el cual ya existen normas que abordan específicamente las situaciones de uso de información personal de las personas con fines comerciales y publicitarios. Es difícil en la medida que la tecnología presente nuevos inventos que permitan obtener mayor información de los usuarios de maneras que hoy en día no es posible imaginarlas.

Con respecto a que Colombia adopte normas de ordenamientos jurídicos como el Europeo para el manejo de los datos personales en aplicaciones publicitarias no solo es probable, sino que es lo más lógico. Si se hace un análisis detallado, la ley 1581 no está muy lejos de los 3 elementos esenciales que se identifican en las normas Europeas. Recapitulando, estos son; la autorización por parte del usuario, la identidad de la empresa o persona que realiza el tratamiento de datos con fines comerciales y la usabilidad de la plataforma para que se pueda ejercer el derecho de hábeas data.

Los primeros dos elementos, se puede decir, que prácticamente se vuelven una constante en todos los momentos en que las empresas o personas jurídicas colombianas están interactuando con la persona o destinatario. Si bien la ley 1581 legisla no solo pensando en los clientes, sino también en proveedores y empleados, el objetivo es el mismo, que haya un consentimiento por parte del destinatario y que siempre exista y sea claramente identificable el responsable de administrar y manejar los datos personales de las personas que se encuentran en sus bases de datos.

Ahora bien, que la usabilidad de la plataforma sea diseñada de la mejor manera posible para que facilite el ejercicio de habeas data para los usuarios no es un elemento que se identifica en la norma colombiana. Este es un requisito de un tipo más técnico que surge a raíz de que muchas empresas crean el botón de aceptar términos y condiciones de las políticas de privacidad de formas que confunden a los usuarios. Profundizando

un poco más en la materia, es posible que eventualmente se diseñe un formato único para las páginas web, por medio del cual las personas pueden ingresar e identificar qué información se tiene de ellos, como pueden modificarla, quienes la tienen, para que la usan y cómo pueden darse de baja de aquella base de datos. En otros escenarios digitales pero que no corresponden exclusivamente a páginas web, casos como llamadas IP, grabaciones de voz y mensajes de texto y/o chats, es posible que se llegase a exigir ese mismo mecanismo a través de una página web.

Con respecto a lo que en párrafos anteriores se había comentado como el reto más complejo para proyectar el fenómeno del uso de datos personales en estrategias comerciales debido a la imprevisibilidad de los desarrollos tecnológicos, vale la pena hacer la siguiente reflexión: El alcance que ha logrado la tecnología para la recolección de información personal de individuos, ha permitido que las empresas recolecten datos privados; como la edad, fecha de cumpleaños, familiares, equipo de fútbol preferido, que estudia, bandas y grupos musicales preferidos, mascotas, páginas web que frecuentan. Los datos anteriores son los más comunes, pero hay información que va a un nivel aún mayor de profundidad en la privacidad de los individuos. Las empresas tienen acceso a las conversaciones en chats y los correos electrónicos, la identidad biométrica de los individuos cuando alguien publica una foto, la cual es considerada un dato sensible, las aplicaciones que hacen seguimiento del estado de salud de las personas permiten recolectar datos médicos. También existen herramientas tecnológicas que permiten seguir y visualizar qué lugares frecuentan los sujetos, cuáles son sus recorridos diarios.

El punto es, que la tecnología ha alcanzado unos niveles muy altos en la capacidad de recolectar información personal y de acceder a la intimidad de los sujetos, la accesibilidad para recopilarla no es exclusivamente de las grandes empresas con

políticas de responsabilidades claras, sino de cualquier sujeto que tenga la capacidad de procesar de forma inteligente aquella información.

Todo el panorama presentado anteriormente se hace con un objetivo y un punto claro, si bien adaptar las normas de un ordenamiento jurídico como el Europeo para encontrarse vigentes en esta materia es una tarea que, a pesar de un par de debates y discusiones en el Congreso, termina siendo algo viable y posible de lograr, por el contrario, el reto de hacer aplicar estas normas es algo que se vuelve más complejo.

En un principio los órganos estatales entrarán a vigilar a las empresas, comenzando por las grandes compañías, y se encargarán de que estas empresas cumplan con todo lo requerido por la ley. Luego entrarán a regular y vigilar a las medianas y pequeñas empresas y ahí seguirán logrando aplicar las normas cuidando los derechos de los usuarios y su información personal. El problema radicará a futuro y en la medida que la tecnología siga avanzando y sea más accesible para todo el mundo. Hoy en día es la Superintendencia de Industria y Comercio, mañana puede ser otro órgano con otro nombre, pero el problema será controlar no solo a las empresas, sino a todas las personas que están haciendo tratamiento de datos personales de otras personas. La protección de los datos personales en sentido estricto, como una obligación que ha asumido el Estado con la expedición de la ley 1581, es y será un reto constante.

No tiene ninguna utilidad crear una norma que sirva para proteger los datos personales de las personas de las grandes corporaciones, si por otro lado no existe la posibilidad de protegerlos de un simple individuo con un computador. Ese panorama simplemente plantearía el caso que la ley se convierte en alguna medida en letra muerta. El Estado deberá diseñar y crear herramientas que permitan las protección de los datos personales de las personas tanto de las grandes compañías como de los negocios informales, sin

embargo y por más que lo intente, esta es un tarea como muchas de las que tiene el Estado, con alto grado de dificultad para cumplir, además que existen otros derechos constitucionales de los Colombianos que requieren más atención y recursos económicos, por parte del Estado antes que al tema de protección de los datos personales.

La importancia de la información y datos personales de los sujetos es un tema que es de gran importancia, y si bien existen algunos derechos constitucionales como la vida, la salud entre otros, que como se mencionó anteriormente, requieren de un mayor esfuerzo por parte del Estado, la información personal de un individuo hace parte esencial de su identidad y su privacidad. Alcanzar un punto óptimo donde el Estado pueda cumplir con este reto, no solo para la publicidad sino para cualquier caso, no es un panorama que se puede ver en el corto plazo, es por este motivo que la estrategia principal que se debe aplicar es la educación. Cabe anotar la observación sobre la naturaleza de los principios que se hace en la Sentencia C-228 de 2011, aludiendo a la terminología de Robert Alexy, “son un mandato de optimización que ordena que se realice algo en la mayor medida de lo posible de acuerdo con las posibilidades jurídicas y fácticas”

Educar a las personas para que hagan un uso responsable de las plataformas digitales, de la información que publican y de lo que están dispuestas a exponer, es la mejor alternativa para abordar el reto a mantenerse vigente en la era digital.

BIBLIOGRAFIA

BONICHOT, J.-C., caso C-192/08 de la Segunda Cámara del Parlamento Europeo. MMS. SMS Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:es:PDF. (Tomado el 6 de enero de 2016)

CARRIER, Jean-Guy y MANFREDI, John F., ICC. Cámara de comercio Internacional. MBHU. Disponible en: http://www.codescentre.com/media/1328/cdigo%20consolidado%20icc%20(1).pdf (Tomado el 17 de febrero de 2016)

CHRISTENSSON, Per. TECHTERMS. Cookie., Disponible en http://techterms.com/definition/cookie. (Tomado el 5 de febrero de 2016)

Constitución Política de 1991. Julio 7 de 1991. Colombia.

Corte Constitucional. Sentencia C – 748 de 2011., (M.P.: JORGE IGNACIO PRETELT CHALJUB).

Corte Constitucional. Sentencia T – 729 de 2002., (M.P.: EDUARDO MONTEALEGRE LYNETT).

GOOGLE. Anuncio flotante. Disponible en: https://support.Google.com/adwordspolicy/answer/176108?hl=es-419 (Tomado el 12 de enero de 2016).

IBOPE, Grupo. Media Colombia. Disponible en: www.Ibope.com/medios.html (Tomado el 5 de febrero de 2016)

LEY ESTATUTARIA 1581 DE 2012. (2012). Por Congreso de Colombia. República de Colombia. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html (Tomado el 14 de febrero de 2016).

LEY 1480 DE 2011. (2011). Por Congreso de Colombia. República de Colombia. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1480_2011.html tomado el 28 de diciembre de 2015.

LUISSANET. Innovación Disruptiva. Disponible en: http://www.luisan.net/blog/marketing/innovacion-disruptiva (Tomado el 28 de febrero de 2016)

MARAZZI, Axel. La Nación. Nube / cloud computing. Disponible en: http://www.conexionbrando.com/1389864-que-es-la-nube-para-que-sirve-y-cuales-son-los-servicios-que-tenes-que-conocer. (Tomado el 18 de febrero de 2016)

NEIRA AVILA, Tito Pablo ACIM. Praxis y Torus. Colombia. Estudio General de Medios. Disponible en: http://www.acimcolombia.com/estudios/estudio-general-de-medios-egm/ Ficha técnica de estudio disponible en: http://www.acimcolombia.com/wp-

content/uploads/2015/07/FICHAEGM2010.pdf (Tomado el 18 de febrero de 2016).

OFCOM. Regulador Independiente y autoridades de Competencia para las Industrias de las Comunicación en el Reino Unido. Publicidad por emplazamiento. Disponible en: http://www.undertv.tv/product_placement.htm (Tomado el 20 de febrero de 2016)

Parlamento Europeo y el Consejo de la Unión Europea. (2001). Reglamento (ce) no 45/2001 del Parlamento Europeo y del consejo de 18 de diciembre de 2000. Bruselas: Diario Oficial de las Comunidades Europeas. (Tomado el 5 de diciembre de 2015)

PARTNER, I. (2015). Practical Law. Us.practicallaw.com., Disponible en http://us.practicallaw.com/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1248063181319&ssbinary=true (Tomado el 15 febrero de 2016).

REMOLINA ANGARITA, Nelson. Revista Latinoamericana de Protección de Datos Personales. Word press. ISSN 2422-6769. Disponible en http://www.rlpdp.com/2012/12/382/ (Tomado el 15 de diciembre de 2015)

SIERRA GARCIA, Manuel. Apr2.com. Servidor. Disponible en: http://aprenderaprogramar.com/index.php?option=com_attachments&task=download&id=487 (Tomado el 25 de diciembre de 2015)

STATISTA. The Statistics Portal. Disponible en: http://www.statista.com/statistics/266249/advertising-revenue-of-Google/ (Tomado el 21 de febrero de 2016).

STATISTA. The Statistics Portal. Disponible en: http://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/ (Tomado el 21 de febrero de 2016).

TARGET GROUP INDEX IBOPE Media Colombia. Disponible en: www.Ibope.com/medios.html (Tomado el 26 de diciembre de 2016)

Tratado Constitutivo de la Comunidad Europea. Tratado de Puerto Seguro. Disponible en: http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/common/B.12-cp--Decisi-oo-n--sobre-la-adecuaci-oo-n-conferida-por-los-principios-de-puerto-seguro.pdf. (Tomado el 6 de enero de 2015)