DATOS PERSONALES EN SITIOS *WEB:* EL CASO DE LAS *COOKIES* EN EL CONTEXTO COLOMBIANO

ANDREA ISABEL BETANCUR ALZATE

VERÓNICA JOHANA MARÍN ALZATE

UNIVERSIDAD EAFIT

ESCUELA DE DERECHO

MEDELLÍN

2020

DATOS PERSONALES EN SITIOS *WEB*: EL CASO DE LAS *COOKIES* EN EL CONTEXTO COLOMBIANO

ANDREA ISABEL BETANCUR ALZATE

VERÓNICA JOHANA MARÍN ALZATE

Monografía presentada para optar al título de Abogado

ASESORA

PAOLA XIMENA MOLINA RINCÓN

UNIVERSIDAD EAFIT

ESCUELA DE DERECHO

MEDELLÍN

2020

Resumen

Es innegable que hoy en día estamos en una era en la cual la tecnología se ha involucrado de manera inherente a la existencia del ser humano. Según los datos suministrados por el operador *Global Web Index*, encargado de generar los *ranking*s mundiales del tiempo invertido en Internet, Colombia es el cuarto país en el mundo en el que las personas permanecen más tiempo navegando (Venegas, 2019). Pero ¿qué implica navegar en la red? Una de las principales consecuencias y, que ha tomado mayor relevancia en la actualidad, es el suministro de datos personales por parte del usuario en diferentes plataformas, redes sociales, y sitios *web*. Así, acceder a determinado servicio supone entregar al mundo digital su huella personal y, con ello, permitir que muchos de los servidores accedan a esta información de forma sencilla e ilimitada.

Así las cosas, una de las maneras de captar esta información es a través de las *cookies.* Estas han adquirido mayor relevancia en la última década, de cara a la función que cumplen en los sitios *web*, al recopilar datos sobre las preferencias, ubicación y hábitos de navegación del usuario. Lo que, en últimas, beneficia en mayor medida al responsable del sitio, pues posibilita ejercer el poder informático sobre el comportamiento en línea de los usuarios.

Bajo este contexto, la presente monografía pretende establecer si la regulación vigente en Colombia sobre protección de datos personales ampara adecuadamente el derecho de *habeas data* frente a los riesgos derivados de su captación a través de las *cookies*. Por lo tanto, se realizará un análisis del régimen de protección de datos personales colombiano y, asimismo, se estudiará la legislación europea semejante, debido a que es un referente internacional que se ha pronunciado de manera reiterada sobre el uso de *cookies* en sitios *web*.

Abstract

It is undeniable that today we live in an era in which technology has been heavily involved in our day to day lives. According to the data provided by the Global *Web* Index operator, in charge of generating the world rankings of the time spent on the Internet, Colombia is ranked fourth in the world on a per capita basis in *web* browsing (Venegas, 2019). But what implications does surfing the *web* have? One of the main consequences, and one that has become more relevant today, is the logging of personal data by users on different platforms, social media, and *web*sites. Thus, accessing a certain service means providing the digital world

your personal fingerprint and, with it, allowing many servers to access this private information in a simple and unlimited manner.

One of the ways to capture this information is through cookies. These have become more relevant in the last decade, they collect data on the user's preferences, location and browsing habits. Which, ultimately, benefits the entity responsible for the site, since it makes it possible to use that information to better understand the online behavior of the users.

In this context, this monograph aims to establish whether the current regulation in Colombia on the protection of personal data properly protects the right to *habeas data* against the risks derived from its capture through cookies. Therefore, an analysis of the Colombian personal data protection regime will be carried out and, likewise, similar European legislation will be studied, since it is an international benchmark that has repeatedly ruled on the use of cookies on *web*sites.

Palabras clave

Datos personales, *cookies*, *habeas data,* derecho a la intimidad, usuario, sitio *web*, tratamiento de datos personales.

Key words

Personal data, cookies, habeas data, privacy right, user, website, processing of personal data.

Tabla de contenido

Tabla de Figuras

INTRODUCCIÓN

Los medios digitales se presentan en el siglo XXI como una de las herramientas más eficientes para satisfacer las necesidades frecuentes. La hiperconectividad y globalización se han convertido en la cotidianidad de las personas, quienes utilizan las Tecnologías para la Información y la Comunicación (TICs) como medio para vivir en sociedad.

Prueba de lo anterior, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic) (2019), mediante el boletín trimestral de las TIC, determinó que para el segundo trimestre del 2019 Colombia contaba con 34.6 millones de conexiones a Internet de Banda Ancha. Esto supone, que 27,7 millones de personas accedieron a Internet a través de dispositivos móviles, mientras que 6,9 millones de personas tuvieron acceso fijo al servicio. Todo esto se traduce en un consumo digital a gran escala, donde el usuario (persona natural que busca información, bienes y servicios) y el prestador de servicios (sitio *web* o navegador *web*) adquieren un papel relevante en la actualidad, al ser los principales actores en las conexiones llevadas a cabo diariamente.

En el intercambio de datos entre sitio *web*, navegador *web* y usuario, los datos personales de este último se podrían propagar a través de muchos medios. Uno de estos son las *cookies*, que permiten almacenar a un sitio *web* cierta información en nuestros dispositivos electrónicos o navegadores *web*. Lo anterior, con el fin de recuperarla y posteriormente utilizarla para reconocer e identificar al usuario, ofrecer servicios, optimizar procesos, mejorar su sitio o analizar su comportamiento. Así, se crea un perfil en línea a partir de la recolección de datos personales y, a su vez, posiblemente, crear una base de datos para identificar fácilmente su género, ubicación, cuáles son sus gustos y, en general, todos sus hábitos en la red.

Con base en lo anterior, cabe preguntarse si los riesgos derivados del uso de las *cookies* frente a los datos personales se pueden mitigar a partir de lo dispuesto en la normatividad colombiana, ya que el fácil acceso a los medios digitales y la necesidad de hacer uso de ellos, llevan a que las personas entreguen libremente su información en los sitios *web*. Esta es utilizada a una escala sin precedentes a la hora de realizar sus actividades, sin saber realmente quiénes los están tratando, con qué finalidad lo están haciendo y si realmente están respetando el derecho de *habeas data*.

En ese orden de ideas, se puede afirmar que a pesar de que la tecnología se ha desarrollado con independencia de la existencia de una regulación previa, no obsta para que el derecho se

encargue posteriormente de regular los avances tecnológicos, con el ánimo de salvaguardar los postulados de un Estado Social de Derecho. En ese contexto, las *cookies* constituyen un claro ejemplo del desarrollo acelerado de la tecnología, aunque no existiese normatividad previa a su creación. Aquellos archivos informáticos creados desde 1994[1] se han convertido en una herramienta esencial para que sitios y navegadores *web* obtengan información sobre los usuarios, dejando a la incertidumbre cuestionamientos como: ¿cuáles son las implicaciones del uso de *cookies* en un sitio *web*? ¿están transmitiendo ilimitadamente nuestros datos a terceros? ¿es posible que nuestros datos perduren indefinidamente en poder del responsable del sitio *web*?

Es importante aclarar que este trabajo no pretende centrarse en el análisis del comercio electrónico, más conocido como *E-commerce*. Tampoco busca analizar el fin publicitario que tienen las *cookies*, sino que se centra en determinar el impacto de estas sobre los datos personales en sitios *web*.

Con base en lo anterior, el objetivo de esta monografía es establecer si la normatividad vigente en Colombia sobre protección de datos personales regula adecuadamente el derecho de *habeas data* frente a los riesgos derivados de la captación de información a través de las *cookies*. Para ello, este texto se estructurará en cinco capítulos de la siguiente forma:

En el primer capítulo, se definirán determinados conceptos relacionados con las *cookies* y sus riesgos frente a los datos personales, los cuales serán indispensables para contextualizar al lector sobre el contenido de la monografía. En el segundo capítulo, se hará un recuento de la jurisprudencia más relevante de la Corte Constitucional respecto de los derechos de *habeas data* e intimidad, con el fin de establecer su protección constitucional e importancia frente a los riesgos derivados del uso de *cookies*. En el tercer capítulo, se analizará la normatividad existente respecto al tema de datos personales, es decir, la Ley Estatutaria 1581 de 2012 y el Decreto 1377 de 2013, para dar a conocer el panorama jurídico vigente en Colombia. Por su parte, en el cuarto capítulo, debido a la inexistencia de normas jurídicas que regulen las *cookies* en Colombia, se realizará un análisis de la legislación sobre datos personales de la Unión Europea como fuente auxiliar. Esto, ya que regula el tema en cuestión, específicamente a

[1] De acuerdo con el profesor de la Universidad de Alicante, Sergio Luján Mora (2011), las *cookies* fueron creadas en 1994 por ingenieros del extinto navegador *Netscape*, con el fin de implementar el carrito de compras virtual. Esto, permitió al usuario guardar los elementos seleccionados, mientras continuaba navegando en el sitio *web*.

través de la Ley 34 de 2002 y la *Guía sobre el uso de las cookies* de la Agencia Española de Protección de Datos Personales (2019) y, de manera general, por medio de la Directiva 58 de 2002 y del Reglamento General de Protección de Datos 679 de 2016. Este análisis se realiza con el fin de brindar un panorama amplio sobre el marco legal de dicho continente, especialmente de España. A su vez, se presentará un estudio sobre la manera como los sitios *web* españoles y colombianos dan a conocer el uso de *cookies* a los usuarios, y así evidenciar sus diferencias. El quinto y último capítulo, buscará detallar los aspectos relacionados con las *cookies* que no estén regulados por la legislación colombiana vigente sobre datos personales y aquellos aspectos regulados pero que necesitan ser precisados. Esto, con el fin de determinar los elementos que posiblemente se requiera introducir o ajustar, en caso de que se legisle sobre el tema en Colombia. Por último, se presentarán las recomendaciones derivadas del análisis realizado previamente, para determinar si es menester crear una regulación de las *cookies* que respete los lineamientos de la Ley de protección de datos personales colombiana o si basta con adecuar la existente.

1. CONCEPTOS FUNDAMENTALES Y RIESGOS DE LA RECOLECCIÓN DE DATOS A TRAVÉS DE LAS *COOKIES*

Este capítulo busca ilustrar al lector sobre los conceptos claves para comprender el contexto en el que se desarrollará la tesis. Posteriormente, se describirán los tipos de *cookies* que, por su naturaleza y funcionamiento,[2] resultan problemáticos frente al tratamiento de datos personales de los usuarios en los sitios *web*. Por último, se analizarán los riesgos que se han identificado a partir de la recolección de información por medio de las *cookies*.

1.1. DATOS PERSONALES

Se entiende por dato personal toda aquella información que se afirma sobre una persona física determinada o determinable. Se considera como persona determinada aquella que se distingue de los demás miembros de un grupo y determinable aquella que, sin estar identificada, se puede llegar a reconocer a través de "características físicas, económicas, culturales, sociales, número de identificación, número de teléfono, dirección de domicilio, dirección IP, entre otras" (Rebollo, 2008, pp 110-111). Se hace la salvedad de que la información que permite determinar a una persona no necesariamente debe estar recogida en una base de datos, ya que también serán datos personales los contenidos en un texto libre, escrito en formato digital, ya sea en una página *web* o en un mensaje de correo electrónico (Oró, 2015, p.53).

1.2. BASES DE DATOS

Las bases de datos son un conjunto organizado de datos que permite obtener con rapidez diversos tipos de información (Real Academia Española, 2014). También se entenderá por base de datos aquella "colección de información organizada de tal modo que sea fácilmente accesible, gestionada y actualizada" (Rouse, 2015).

1.3 PÁGINAS *WEB*, SITIOS *WEB* Y NAVEGADORES *WEB*

La página *web* es aquel documento electrónico que contiene información digital y forma parte de un sitio *web*. Suele contar con enlaces como hipervínculos o *links* para permitir una navegación más sencilla al usuario.

[2] El término funcionamiento, en adelante, hará referencia a todo el proceso que se lleva a cabo para captar datos a través de las *cookie*s, esto es, desde la solicitud que hace un navegador *web* a un servidor para instalarlas, hasta el contenido que estas recopilan.

El sitio *web* es aquel espacio virtual conformado por una colección de archivos electrónicos o páginas *web* a las cuales se puede acceder a través de un mismo dominio en Internet, o más específicamente en la *World Wide Web* (*www*).

Un ejemplo que permite ilustrar al lector sobre la diferencia entre el primero y el segundo es el siguiente: la Universidad EAFIT cuenta con un sitio *web* identificado a través de la siguiente dirección http://www.eafit.edu.co/, cada sección dentro de este sitio, por ejemplo "Estudiar en EAFIT", "Academia", "Investigación", "Proyección", son las páginas *web*. En últimas, la *World Wide Web* estaría conformada por innumerables sitios *web* y estos a su vez por páginas *web*.

Por otra parte, un navegador *web* es aquel programa o *software* que permite acceder a diferentes sitios y páginas *web* para visualizar la información incorporada como imágenes, videos, archivos, entre otros. Así, los navegadores más conocidos son: *Google Chrome*, Internet *Explorer*, *Mozilla Firefox* y *Safari.* En este sentido, un sitio *web* es un conjunto de páginas *web* referidos a un mismo tema en particular; mientras que un navegador *web* es un programa o *software* que permite el acceso a Internet y el ingreso a diferentes sitios y páginas *web*.

1.4. *COOKIES*

La *Guía sobre el uso de las cookies de la* Agencia Española de Protección de Datos (AEPD), define las *cookies* como: "cualquier tipo de dispositivo de almacenamiento y recuperación de datos que se utilice en el equipo terminal de un usuario con la finalidad de almacenar información y recuperar la información (sic) ya almacenada" (Agencia Española de Protección de Datos [AEPD] 2019, p.11). En otras palabras, son documentos que contienen información sobre los hábitos de búsqueda, ubicación, idioma, usuario en línea y contraseña del usuario que accede al sitio *web*. Dicha información recaudada se almacena en el navegador *web* o disco duro del dispositivo electrónico con el que se ingresa a Internet. Lo anterior, con el fin de facilitar la navegación del usuario en caso de que requiera visitar nuevamente el sitio. En consecuencia, tanto sitios como navegadores *web* tendrán acceso a los datos recaudados a través de las *cookies*.

Como se lee en la definición presentada, las *cookies* no son malas *per se*, simplemente son un protocolo utilizado en Internet que ayuda a generar interacción y/o comunicación entre servidores y usuarios. Esto facilita, por un lado, la experiencia del usuario con base en sus

necesidades y, por otro, brinda a los sitios *web* información sobre las preferencias del cibernauta, para así mejorar sus bienes y servicios.

Un ejemplo que ilustra dicha situación, es cuando un usuario quiere acceder al sitio *web* cuyo nombre de dominio es https://www.eafit.edu.co/. Para ello, ingresa al navegador *web* y lo escribe en el buscador. Este navegador se conectará con el servidor[3] y realizará una petición *http*. El servidor responderá al navegador enviando una respuesta *http* que, además de contener el sitio *web* solicitado, añadirá una serie de códigos para que el navegador los almacene. Estos códigos corresponden a las *cookies.* En consecuencia, cuando el usuario vuelva a ingresar al mismo sitio *web*, el navegador enviará la petición *http,* junto con las *cookies* que ya estaban almacenadas y contenían los datos del usuario. Es a partir de esta acción que los sitios comienzan a crear un perfil en línea del usuario.

Así las cosas, las *cookies* enviadas por el servidor al navegador se componen de: primero, el nombre de la *cookie*; segundo, el nombre de dominio en el que se almacena, siendo el único en el que se pueden emplear la(s) *cookie*(s); tercero, una ruta para limitar el uso de la *cookie* a las páginas dispuestas en ella; cuarto, una fecha de creación y de caducidad; quinto, "solo conexión segura", obligando a enviar la *cookie* mediante un protocolo de encriptación y, por último, el término "solo *http*" para limitar el uso de la *cookie* a dicho protocolo (Universidad de Alicante, 2011).

Adicionalmente, aunque existen diversos tipos de *cookies,* se definirá aquellos que por su naturaleza y funcionamiento pueden resultar problemáticos frente al tratamiento y uso de datos personales. Entre estos, se encuentran: las *cookies* propias, de terceros, de preferencias o personalización, de publicidad comportamental, de sesión y persistentes. Cabe resaltar que esta clasificación no es excluyente, ya que dentro de un mismo sitio *web* pueden coexistir diversidad de éstas. Por lo tanto, una *cookie* puede cumplir al mismo tiempo diferentes finalidades, por ejemplo, técnica, persistente y de publicidad comportamental simultáneamente, a esta clase de *cookies* se le denomina *cookies* polivalentes.

[3] Un servidor *web* es un "programa u ordenador con programas capaces de ofrecer a clientes determinados servicios, tales como correo electrónico (e-mail), transferencia de ficheros (ftp) o páginas Web (http)" (De Andrés, 2005). También se puede entender como servidor "Unidad informática que proporciona diversos servicios a computadoras conectadas con ella a través de una red" (RAE, 2014).

- ***Cookies* propias:** son aquellas que genera directamente el sitio *web* ingresado por el usuario. Por ejemplo, si un cibernauta ingresa al sitio *web* de El Espectador, las *cookies* propias solo serán las generadas por este.
- ***Cookies* de terceros**: son aquellas generadas por otros sitios *web* diferentes al accedido. Estas *cookies* generalmente se instalan a través de anuncios que recogen información como la ubicación, la edad, el sexo y el comportamiento del usuario. Lo anterior, permite su uso como herramientas de rastreo para ayudar al *marketing* y a la publicidad, en general, de cada uno de los servidores donde se alojan las *cookies*. (Digital Guide Ionos, 2018). A su vez, realizan un seguimiento de cada uno de los movimientos que los usuarios hacen en Internet, observan su comportamiento, identifican sus intereses y, a partir de esto, construyen un patrón de consumo para crear perfiles y generar publicidad personalizada.
- ***Cookies* de preferencias o personalización:** "Son aquellas que permiten recordar información para que el usuario acceda al servicio con determinadas características que pueden diferenciar su experiencia de la de otros usuarios" (AEPD, 2019, p. 12). Estas guardan información sobre las distintas elecciones que realiza el cibernauta, tales como: el idioma, la región, el tipo de navegador, entre otras.
- ***Cookies* de publicidad comportamental:** son aquellas *cookies* que "almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo" (AEPD, 2019, p. 12). De esta manera, posibilitan el uso de parámetros de eficiencia en la publicidad ofrecida en los sitios *web*, conforme al comportamiento en línea de los usuarios, para conocer sus intereses.
- ***Cookies* de sesión:** se usan para almacenar datos mientras el usuario permanezca en un sitio *web* y desaparecen cuando el usuario termine la sesión. "Se suelen emplear para almacenar información que solo interesa conservar para la prestación del servicio solicitado por el usuario en una sola ocasión (por ejemplo, una lista de productos adquiridos) y desaparecen al terminar la sesión" (AEPD, 2019, p. 13). Estas *cookies* permiten que el usuario, una vez ingrese a un sitio *web* y se registre, sea reconocido para que, en caso de que introduzca un dato en su cuenta o agregue un artículo a la lista de productos adquiridos (carrito de compras), sea recordado mientras se encuentre navegando en el sitio *web*. Por lo tanto, una vez este cierre la sesión, expiran y son borradas del dispositivo.

- ***Cookies* persistentes:** son aquellas que se almacenan en el navegador o dispositivo del usuario durante el tiempo requerido por el sitio *web*, para cumplir con la finalidad por la cual se instalaron, y expiran al momento de ejecutarlo. Se incorporan y son tratadas por el responsable de las *cookies* durante un periodo que puede durar minutos o varios años, pero que, en todo caso, pueden ser borradas del navegador manualmente por el usuario para que dejen de recibir información sobre su navegación (BBC Mundo, 2017).

1.5 RIESGOS DE LA IMPLEMENTACIÓN DE LAS *COOKIES* FRENTE A LOS DATOS PERSONALES

We Are Social and Hootsuite, en el estudio *Digital 2020 Global Digital Yearbook* (2020) asegura que cerca de 35 millones de colombianos son usuarios de Internet, los cuales comparten datos, interactúan día y noche, y dejan incontables huellas digitales. Esas huellas digitales son traducidas en lo que hemos denominado *cookies*; hoy más que nunca los avances logrados son más visibles en los últimos años: sus usos e incursión en la creación y revolución del mercado electrónico o anuncios *online*. Estas se han multiplicado y toman caminos diferentes según los intereses particulares de los responsables y encargados de hacer su tratamiento.

Ahora bien, en Colombia no existe una regulación específica de estos archivos informáticos. Por eso, los sitios *web* a los que se accede en este país no tienen la obligación legal de proveer al usuario información acerca de las *cookies*. No obstante, en muchos de los sitios *web* se encuentran anuncios, *banners* o *covers*,[4] con un aviso de *cookies* para obtener la aceptación de operar estas herramientas mientras se navegue en dicho sitio. Esto, con el fin de mejorar su funcionamiento y la experiencia del usuario, a través de la captación de información que les permita a los responsables no solo obtener datos estadísticos sobre sus visitantes o clientes, sino además obtener sus preferencias y gustos para ofrecer lo que buscan.

En los casos en los que el sitio *web* dispone de este anuncio, por lo general solicita la autorización del funcionamiento de las *cookies* a partir de un *"clic"* en el botón que indica "aceptar", "estar de acuerdo" o "permitir" las *cookies*. Botón que muchas veces es pulsado para acceder al contenido ofrecido en el sitio *web*, mas no porque haya una consciencia sobre lo que significa "aceptar las *cookies*". Tal como lo ejemplifican *Smit, Van Noort y Voorveld*

[4] Formato gráfico en cuadro, barras y círculos para la divulgación de una información dentro de un sitio *web* o un en vivo en diferentes plataformas digitales.

(2014), en Europa, a gran parte de los ciudadanos les preocupa que se use su información personal, por terceros, sin su consentimiento, debido a que desconocen el funcionamiento dado a las *cookies* e incluso desconocen de su existencia (Smit,Van Noort y Voorveld, 2014, como se citó en Carmi, 2017, pp. 302-303). Lo anterior, demuestra que es un tema inquietante para muchas personas en el mundo, pues tiene una repercusión más allá de Colombia y causa inseguridad frente a la información recogida en el sitio *web* cuando se explora.

Con base en lo anterior, la existencia de riesgos es inminente a la hora de tratar datos personales, debido a la constante transformación del entorno digital y a la evolución de programas tecnológicos para identificar mejor al usuario. Así, dichas circunstancias ponen en riesgo la protección efectiva de derechos fundamentales como la intimidad y el derecho de *habeas data*. Sin duda, su vulneración puede llegar a suponer la afectación de otros derechos.

En este sentido, existen riesgos a la hora de analizar el funcionamiento de las *cookies*. Newman y Ángel (2019) identifican los siguientes, derivados de la utilización dada por los sitios *web* a las *cookies:*

1. No se puede determinar con certeza qué tipos de datos o información captan las *cookies*, ya que no todos los sitios *web* cuentan con aviso o Política de *cookies* que establezca los archivos implementados para ello. Por otro lado, los sitios *web* con dicho aviso, normalmente no describen en detalle la clase de información obtenida. Por lo tanto, el usuario no tiene control sobre sus datos recolectados.
2. No se puede delimitar cuál es el nivel de protección que están implementando los sitios *web* al momento de tratar y conservar los datos personales. Esto, debido a que, una vez el usuario autorice el uso de *cookies*, no hay suficiente claridad frente al proceso para conocer sobre el tratamiento de sus datos personales, esto es, el ejercicio de su derecho de *habeas data*.
3. En muchos casos no se proporciona información suficiente al titular sobre la finalidad por la cual se están utilizando las *cookies*. Por lo tanto, están sujetos a decisiones inciertas y sin un control propio.
4. La inexactitud de los datos captados por las *cookies* instaladas en los sitios *web puede* conllevar a actos de discriminación, los cuales ponen en riesgo el derecho a la intimidad del individuo.
5. El manejo dado a las *cookies* en los sitios *web* por terceros. Esta situación implica una gran pérdida de confianza por parte de los usuarios, ya que los datos personales

depositados en un sitio *web*, pueden ser transferidos de manera ilimitada a terceros que ni siquiera conocen.

6. Creación de perfiles en línea, ocultando al usuario esta situación. La perfilación puede aumentar la segregación social, discriminación injustificada, además de violentar la libertad de las personas para elegir productos o servicios, al restringirlos a sus preferencias.

Ahora bien, teniendo en cuenta los riesgos existentes de cara al funcionamiento de las *cookies* la pregunta a realizar es: ¿qué alternativas existen para reducir los riesgos que se derivan del uso de estas? Una posibilidad, es la limitación del uso de las *cookies* de terceros. Según el periódico La República en el artículo escrito por Bloomberg (2020), *Google* -uno de los navegadores más importantes del mundo- restringirá los diferentes usos de este tipo de *cookies*, ya que los datos de muchos usuarios se captan para un fin no esperado, vulnerando con ello su derecho de *habeas data*. Esto hizo que *Google* decidiera que, dentro de dos años, dejará de admitir las *cookies* de terceros para garantizar a los usuarios su privacidad, poder de decisión y control sobre cómo se utilizan sus datos. No obstante, aunque es una decisión ya adoptada por otros navegadores como *Safari* y *Mozilla Firefox*, representa un gran cambio para el *marketing* digital al ser *Chrome* el navegador *web* más utilizado en el mundo (Expansión, 2018).

De acuerdo con esta noticia, para Ari Paparo, jefe de la firma de publicidad digital *Beeswax* y exejecutivo de *Google*, restringir las *cookies* cambia la forma de hacer publicidad, ya que estas permiten realizar ofertas con base en algoritmos (Bloomberg, 2020). Lo anterior, implicará innovar en la manera como se hará la publicidad dirigida en los sitios *web*, y a su vez, el desarrollo de técnicas especiales para detectar, reducir el seguimiento y la intrusión en la privacidad de los usuarios en Internet (Schuh, 2020).

2. JURISPRUDENCIA CONSTITUCIONAL: DERECHOS CONSTITUCIONALES

En el presente capítulo se realizará una cronología sobre la consagración jurisprudencial del *habeas data*, pues este derecho ha tenido una evolución significativa desde la Constitución Política de 1991. Esto, dado que cada pronunciamiento del Tribunal Constitucional ha moldeado y delimitando no solo su definición y núcleo esencial, sino también sus mecanismos de protección, como la acción de tutela, principios, lineamientos y situaciones en que se vulneran. Igualmente, se realizará un breve recorrido de la jurisprudencia más relevante de la

Corte Constitucional sobre el derecho fundamental a la intimidad, pues encuentra relación directa con los datos personales.

De esta manera, se analizará el contenido y las disposiciones más relevantes, sin pretender hacer líneas jurisprudenciales. Estos fallos deben ser tenidos en cuenta por parte de los Responsables y encargados del tratamiento de los Datos Personales para garantizar la protección de estos derechos y evitar posibles vulneraciones a través del funcionamiento de las *cookies* en sitios *web*.

2.1 DERECHO DE *HABEAS DATA*

El derecho de *habeas data* se consagró desde la Constitución Política de 1991 en su artículo 15 estableciendo que:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas (Constitución Política de Colombia [Const.], 2015, p. 11).

Desde ese entonces, la Corte en la Sentencia T-414 de 1992 (1992), señaló de manera breve algunos aspectos de la disposición constitucional que consagra el derecho de *habeas data*, en la que el Constituyente buscó proteger la honra y libertad contra los abusos del poder informático. Así, en este primer pronunciamiento, la Corte determinó que el derecho de *habeas data* garantiza el derecho a la intimidad, pues la persona es la única con derecho a divulgar información de su vida privada (Sentencia T-238/2018, 2018), por lo que:

> Toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada. Su finalidad es la de asegurar la protección de intereses morales; su titular no puede renunciar total o definitivamente a la intimidad pues dicho acto estaría viciado de nulidad absoluta (Sentencia T-414/1992, 1992).

Este planteamiento se sostuvo en pronunciamientos posteriores, como en la Sentencia T-525 de 1992, la Sentencia T-444 de 1992 y la Sentencia T-022 de 1993, en las cuales la Corte

consideró que el derecho de *habeas data* se encontraba dentro de una de las dimensiones del derecho a la intimidad. Este último hacía referencia, en primer lugar, al derecho a obtener información personal dispuesta en archivos o bases de datos, en segundo lugar al derecho a ser informado sobre los datos registrados sobre uno mismo, e igualmente comprendía la facultad de corregirlos, difundirlos y, en caso de que existiera, la prohibición de manipular dicha información (Sentencia T-036/2016, 2016). Asimismo, en dichas sentencias la Corte indicó que el fundamento tanto del *habeas data* como de la intimidad era la autodeterminación y la libertad que el ordenamiento jurídico reconoce a las personas en virtud del libre desarrollo de la personalidad y de la dignidad humana.

No obstante, con la Sentencia T-340 de 1993, la Corte desarrolló una segunda interpretación del derecho de *habeas data* como manifestación del libre desarrollo de la personalidad.[5] Lo anterior, se justifica en la medida en que el *habeas data* se fundamenta en la autodeterminación y la libertad de los sujetos para propender por el libre desarrollo de su personalidad (Sentencia T-022/1993, 1993). Por esto, en el evento en el que alguien quiera investigar o divulgar información sobre la vida de una persona, debe solicitar su autorización o tener un interés general legítimo para ello.

Sin embargo, esta postura se sostuvo hasta 1995,[6] año a partir del cual la Corte Constitucional consideró que se debían diferenciar los derechos a la intimidad y al *habeas data*, ya que el Artículo 15 constitucional los consagra, junto con el derecho al buen nombre, como derechos autónomos y distintos (Sentencia T-238/2018, 2018).

Así, la Corte Constitucional, en la Sentencia SU-082 de 1995 (1995), determinó que el núcleo esencial del *habeas data* se compone de: el derecho a la autodeterminación informática, la libertad y la libertad económica. En este sentido, el primer derecho enunciado corresponde a la facultad que tiene la persona titular[7] -sujeto activo del derecho, bien sea natural o jurídica- de autorizar a cualquier persona, natural o jurídica (sujeto pasivo), que utilice sistemas

[5] Aunque así lo indican las Sentencias C-748 de 2011 y T-238 de 2018, realmente la Sentencia T-022 de 1993 fue de las primeras en adoptar esta segunda interpretación del derecho de *habeas data* como condición para el libre desarrollo de la personalidad.
[6] Con la Sentencia SU-082 de 1995, la Corte desarrolló una tercera línea interpretativa: *habeas data* como derecho autónomo.
[7] En ese entonces, se hacía referencia a los datos sobre la capacidad económica de la persona, especialmente lo referente a la forma como cumple con las obligaciones económicas frente a las instituciones de crédito.

informáticos para la conservación, uso y circulación de sus datos personales (Sentencia T-657/2005, 2005). Lo anterior, implica que el titular del dato personal tenga la potestad de decidir en qué momento y bajo qué límites da a conocer situaciones de su vida, exigiendo de las demás medidas de protección frente a la elaboración de un perfil que pueda limitar su poder decisorio. En otras palabras, es el poder exigir un adecuado tratamiento de la información que la persona decidió exhibir a los demás (Sentencia T-552/1997, 1997).

En cuanto a la libertad, en la Sentencia T-303 de 1993 (1993), dispuso que es una facultad del titular de los datos recolectados o transferidos y, así, comprende su fuero interno. Esto es, se permite la recolección, tratamiento y circulación de datos, cuando no se vulnere el derecho a la intimidad que, para ese entonces, contenía al *habeas data*. Por tal motivo, las entidades privadas y públicas que manejan los bancos de datos deberán actuar con el máximo grado de diligencia y razonabilidad, además de respetar la libertad y garantías constitucionales consagradas en el inciso segundo del Artículo 15 constitucional.[8]

La libertad económica, por su parte, se consagró en el artículo 333 de la Constitución Política, que reza:

> La actividad económica y la iniciativa privada son **libres**, dentro de los límites del bien común. Para su ejercicio, nadie podrá exigir permisos previos ni requisitos, sin autorización de la ley.
>
> La libre competencia económica es un derecho de todos que supone responsabilidades.
>
> La empresa, como base del desarrollo, tiene una función social que implica obligaciones. El Estado fortalecerá las organizaciones solidarias y estimulará el desarrollo empresarial.
>
> El Estado, por mandato de la ley, impedirá que se obstruya o se restrinja la **libertad económica** y evitará o controlará cualquier abuso que personas o empresas hagan de su posición dominante en el mercado nacional.
>
> La ley delimitará el alcance de la **libertad económica** cuando así lo exijan el interés social, el ambiente y el patrimonio cultural de la Nación.[9] (Const., 2015, p. 130)

[8] El cual reza: "En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución" (Const., 2015, p. 11).
[9] La negrilla corresponde a las autoras del texto.

A pesar de que la definición del concepto de libertad económica resulta ser problemática por ser una cláusula amplia e indeterminada en el texto Constitucional, al no definirla con claridad (Sentencia C-616/2001, 2001), la Corte Constitucional ha delimitado su alcance desde los primeros fallos. En este sentido, ha interpretado que, de acuerdo con la doctrina, es "una facultad que tiene toda persona de realizar actividades de carácter económico, según sus preferencias o habilidades, con miras a crear, mantener o incrementar un patrimonio." (Sentencia T-425/1992, 1992). Asimismo, ha considerado que la actividad económica es una garantía extendida por igual tanto a empresas legalmente constituidas como a personas naturales y, a su vez, contiene la libertad económica.

Ahora bien, esta libertad forma parte del núcleo esencial del derecho de *habeas data*, debido a que el tratamiento de datos personales representa un interés en dos sentidos: por un lado, para el titular que busca el respeto de sus datos y, por otro, para la economía, ya que si se busca ser un agente económico activo, se requiere suministrar cierta información sobre sí mismo. En este sentido, el *habeas data* constituye un limitante para quien administra los datos personales suministrados por su titular, pues le impone la obligación de protegerlos. Por consiguiente, la Sentencia SU-082 de 1995 (1995) determina que la libertad económica podría vulnerarse si se circulan datos falsos o que no hayan sido autorizados por su titular o por la ley.

Por su parte, la Sentencia T-238 de 2018 (2018) indicó que el Tribunal Constitucional estableció, en la reiterada sentencia de unificación jurisprudencial de 1995, que el *habeas data* contiene tres facultades: primero, el derecho a conocer la información acerca de su titular, segundo, el derecho a actualizarla y, tercero, el derecho a rectificar las informaciones que no sean veraces. No obstante, la Corte reconoció que existen otras facultades no expresadas en el artículo constitucional, como el derecho a la caducidad del dato negativo (información desfavorable sobre el dato financiero) y la exclusión de datos pertenecientes a la esfera íntima del individuo.

Continuando el recuento histórico acerca de este derecho, el Tribunal Constitucional en la Sentencia T-176 de 1995 (1995) determinó que se vulnera el derecho de *habeas data* en tres ocasiones: primero, cuando la información sobre una persona es recolectada de manera ilegal, al no contar con su consentimiento, segundo, cuando esa información es errónea y, tercero, cuando la información hace parte de la intimidad de su titular y, por ende, no debe ser conocida

públicamente. A partir de lo anterior, la Corte entendió que no se constituye una lesión a este derecho fundamental cuando se suministran datos veraces previamente autorizados por su titular.

Posteriormente, señaló que los mecanismos de protección con los que cuenta la persona son la rectificación y la actualización. La rectificación consiste en que el dato coincida con la realidad; la actualización es la verificación de la vigencia del dato y su correspondencia con la realidad (Sentencia T-527/2000, 2000). En este aspecto, la Corte en el año 2002, por medio de la Sentencia T-729 de 2002 (2002), amplió las facultades del titular de la información personal, ya que, al tenor de su interpretación, este puede exigir a las administradoras de bases de datos: el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de la información, e inclusive, puede limitar su divulgación, publicación o cesión. Lo anterior, da cuenta de un avance frente al contenido de este derecho fundamental.

Además, en dicha providencia, Sentencia T-729/2002 (2002), la Corporación compiló los principios desarrollados por la jurisprudencia en los casos de tutela de *habeas data*, con el fin de que la administración de los datos personales se base en: la libertad, necesidad, veracidad, integridad, incorporación, finalidad, utilidad, circulación restringida, caducidad e individualidad.[10] Tales principios procuran por el equilibrio entre los derechos a la información y a la autodeterminación informática.

Es evidente entonces, que el desarrollo jurisprudencial de este derecho ha permitido, inclusive, la expedición de Leyes Estatutarias que regulan el tema específicamente: la Ley 1266 de 2008 y la Ley 1581 de 2012. La primera, reguló parcialmente el derecho de *habeas data*, al enfocarse únicamente en el *habeas data* financiero[11] y, tal como se indicó en la sentencia que analizó la constitucionalidad del Proyecto de Ley Estatutaria, Sentencia C-1011 de 2008, esta norma se concentró en el funcionamiento y reglamentación de la administración de datos personales de índole financiera y comercial que son usados para calcular el riesgo crediticio. Por lo anterior, se excluyó cualquier otro tipo de datos personales. Sin embargo, la presente monografía no analizará esta Ley, pues la atención se centrará en la Ley 1581 de 2012, que determinó aspectos generales de la protección de datos personales.

[10] Principios que se desarrollarán más adelante en el Capítulo 3 sobre la legislación colombiana.

[11] Según la Sentencia C-1011 de 2008 (2008) es "el derecho que tiene todo individuo a conocer, actualizar y rectificar su información personal comercial, crediticia y financiera, contenida en centrales de información públicas o privadas, que tienen como función recopilar, tratar y circular esos datos con el fin de determinar el nivel de riesgo financiero de su titular."

Esta Ley Estatutaria de 2012 se expidió luego de que la Corte hubiera estudiado la constitucionalidad del Proyecto de Ley a través de la Providencia C-748 de 2011. En ella, determinó que dicha norma introdujo principios y reglas generales, garantizando contenidos mínimos del derecho de *habeas data*. Además, introdujo conceptos claves sobre protección de datos personales, como lo son: bases de datos, tratamiento de datos personales y archivos.[12] Estos son de utilidad para la presente monografía, por cuanto las *cookies* son pequeños archivos que crea un sitio *web* y que son almacenados en el navegador o dispositivo usado por el usuario, los cuales pueden contener datos personales cuya regulación está expresa en esta norma.

Por otra parte, la Corte señaló que los principios plasmados en dicho Proyecto de Ley, se ajustaban no solamente a los lineamientos jurisprudenciales, sino también a los sistemas de protección de derechos internacionales, como: el universal, a través de la Resolución 45/95 de la Organización de las Naciones Unidas (ONU),[13] y los regionales, a través de la Directiva 95/46/CE[14] (en el ámbito europeo), y el *Proyecto de principios y recomendaciones preliminares sobre la protección de datos* realizado por el Departamento de Derecho Internacional de la Secretaría de Asuntos Jurídicos del Consejo Permanente de la Organización de Estados Americanos (OEA) (en el ámbito interamericano). Los anteriores instrumentos incentivan el uso de principios y directrices mínimas que regulan el manejo de datos.

En pronunciamientos más recientes, la Corte Constitucional ha reiterado que las personas jurídicas también son titulares del derecho de *habeas data*, tal como reza el Artículo 15 Constitucional, en el que no se hace distinción entre personas naturales y jurídicas (Sentencia T-238/2018, 2018). De igual manera, reiteró las reglas jurisprudenciales sobre la clasificación de los tipos de información: primero, se clasifican según su capacidad de divulgación como información pública, privada, reservada y semiprivada; segundo, la información semiprivada se refiere a la información personal o impersonal que no sea pública y sobre la cual la sociedad pueda tener un interés legítimo, cuyo acceso sea a partir de una orden judicial o administrativa;

[12] Entendidos como depósitos ordenados de datos que son recolectados, almacenados y usados.
[13] Resolución que determinó principios orientadores de la regulación de ficheros computarizados de datos personales, esto es, archivos de datos personales informatizados.
[14] Directiva que sistematizó las directrices en el manejo de los datos y organizó los principios rectores de acuerdo con la calidad del dato y la legitimidad en su manejo.

tercero, cuando se solicite el acceso a información semiprivada, no se pueden aplicar las reglas sobre reserva de la información pública, como la dispuesta en el Artículo 74 Constitucional y, cuarto, la divulgación o entrega de información semiprivada, debe cumplir con el principio de finalidad del *habeas data*.

Por último, la Sentencia SU-182 de 2019, enfatizó en que el derecho de *habeas data* tiene una doble connotación: como derecho autónomo y como garantía de otros derechos. Así, cumple con el primer fin conforme a lo descrito en párrafos antecedentes y, con el segundo, en la medida en que protege diversos derechos a través de la vigilancia y cumplimiento de las reglas y principios de la administración de datos. Lo anterior, se evidencia por la Corte de la siguiente manera:

> En cuanto al buen nombre, cuando se emplea para rectificar el tratamiento de información falsa, en cuanto al derecho a la seguridad social, cuando se emplea para incluir información personal necesaria para la prestación de los servicios de salud y de las prestaciones propias de la seguridad social, o en cuanto al derecho de locomoción, cuando se solicita para actualizar información relacionada con la vigencia de órdenes de captura (Sentencia SU-182/2019, 2019).

Adicionalmente, el Tribunal Constitucional indicó que el derecho fundamental de *habeas data* supone una obligación correlativa de las entidades públicas y privadas, de responder de manera adecuada y bajo el principio de buena fe, a las solicitudes de acceso, custodia y corrección de la información (Sentencia T-238/2018, 2018).

Finalmente, las decisiones de la Corte Constitucional, en relación con el derecho de *habeas data,* adquieren importancia en el análisis del funcionamiento de las *cookies*, ya que este derecho posibilita a los usuarios el control sobre la información recopilada sobre sí mismos en los sitios *web* accedidos. Lo anterior, se comprende a partir de la manera cómo funcionan las interacciones en Internet, debido a que la información compartida "conserva las memorias" de las acciones realizadas por los usuarios en la *web*: las transacciones electrónicas, los sitios visitados y, en general, su navegación. De este modo, facilita la creación de perfiles a partir de los hábitos de consumo y preferencias.

Así, como consecuencia de que dichas conductas son registradas por las *cookies*, se requiere que el usuario esté facultado para decidir cuándo y cómo compartir sus datos personales,

máxime cuando a partir de ellos se elaboran los perfiles anteriormente mencionados. Esto ocurre, por ejemplo, con las *cookies publicitarias* que analizan los hábitos de navegación de los usuarios para gestionar la publicidad dirigida, y a su vez, para la toma de decisiones automatizadas[15]. Sin embargo, por lo general, dichos tratamientos no son comunicados a los titulares y pueden vulnerar derechos como la autodeterminación informática y el *habeas data*. Por ende, tanto responsables como encargados, deberán garantizar las medidas de protección necesarias, para evitar estos y otros riesgos, como los descritos en la sección 1.5 de este trabajo.

En conclusión, en vista de este contexto, es menester fijar criterios para delimitar el tipo de información compartida con otros agentes en Internet, ya sean entidades estatales o particulares. Esto, debido a que involucra el contenido y alcance del derecho de *habeas data* y de otros derechos relacionados con los datos personales de los usuarios.

2.2 DERECHO A LA INTIMIDAD

A continuación, se realizará un análisis de la jurisprudencia más relevante en torno al derecho fundamental a la intimidad, con base en los pronunciamientos de la Corte Constitucional. Estos han delimitado progresivamente su definición, alcance, niveles de protección y principios. En este sentido, dicho estudio se llevará a cabo teniendo en cuenta las sentencias más recientes de la Corte, en las que se evidencia la evolución de este derecho, y los textos denominados *El derecho a la intimidad y su disponibilidad pública* (Bautista, 2015), y *Derecho a la intimidad y habeas data* (Cervantes, 2009).

En principio, es menester resaltar que el derecho a la intimidad está consagrado en cinco artículos de la Constitución Política de 1991, a saber: 15, 21, 28, 33 y 74. El primero, se refiere a la intimidad bajo la forma de protección de la vida privada y sus implicaciones; el segundo, regula el derecho a la honra; el tercero, consagra la inviolabilidad del domicilio; el cuarto, establece la prohibición de obligar a una persona a declarar contra sí o contra sus seres queridos, y por último, el Artículo 74 dispone el acceso de los particulares a los documentos públicos y el secreto profesional.

[15] Este tratamiento se explicará y desarrollará en los Capítulos 4 y 5 de la presente monografía.

La Corte Constitucional, en la Sentencia T-011 de 1992, estableció que el derecho a la intimidad, dispuesto en el Artículo 15 Constitucional, es expresión del libre desarrollo de la personalidad, cuyo fundamento es la dignidad de la persona. Lo anterior, significa que, al proteger la intimidad, se asegura la paz y tranquilidad necesaria para el desarrollo físico, intelectual y moral, tal como lo señala la Sentencia T-414 de 1992. A partir de este fallo, se determinó que este derecho busca proteger la vida privada del individuo y la de su familia de las injerencias ajenas que, de manera indebida, intervienen en el entorno personal o familiar.

A su vez, indicó que la intimidad es un derecho absoluto, extrapatrimonial, inalienable e imprescriptible y que se puede exigir frente al Estado y a los particulares. Por consiguiente, toda persona es titular de este derecho, y será el único legitimado para difundir los datos concernientes a su vida privada, asegurando la protección de sus intereses. Sin embargo, cabe señalar que no se puede renunciar totalmente a la intimidad, pues dicho acto estaría viciado de nulidad absoluta (Sentencia C-640/2010, 2010).

De igual forma, la Corte resaltó la importancia de controlar el poder sobre la información en el siglo XX y su implicación en el derecho a la intimidad. Así, estableció la necesidad de comprender el dato como un elemento de la identidad de una persona y su combinación con otros puede configurar un "perfil". Este se traduce en lo denominado como "persona virtual", sobre la cual se ejerce un dominio y control social. Conllevando a un desequilibrio entre el poder informático y la intimidad en los países que carecen de una legislación específica que la proteja frente a este (Sentencia T-414 de 1992).

En la Sentencia T-340 de 1993, la Corte reiteró que el derecho a la intimidad permite a toda persona excluir del conocimiento público aquellas situaciones que, por su esencia o por su voluntad, deben mantenerse en la esfera privada de quien los realiza, con el fin de garantizar el ejercicio de este derecho fundamental. Por lo tanto, es obligación del Estado y de los particulares respetarlo y garantizarlo, permitiendo que la vida privada continúe siendo privada, según el deseo de cada persona. Sin embargo, aquella privacidad estará limitada en dos situaciones: primero, cuando el Estado en ejercicio de su potestad inquisitiva inicie investigaciones respecto a determinado sujeto; segundo, cuando los particulares en ejercicio del derecho a la libertad de información, y amparados en el interés público, ponen en conocimiento de la población situaciones de la vida privada de personas que, por razón de sus

ocupaciones, llevan una vida de interés social. Esta excepción no se aplicará si se vulnera el derecho a la intimidad o se atenta contra otro derecho constitucional.

Posteriormente, la Corte en la Sentencia T-176 de 1995 estableció que el derecho a la intimidad es diferente del derecho de *habeas data*, tal como se explicó en la sección 2.1 de la presente monografía. Lo anterior, implicó un gran cambio tanto en la protección judicial por vía de tutela, como en el régimen jurídico aplicable, en caso de que colisione con el derecho a la información, e igualmente la delimitación de los contextos en los que se desarrollan estos derechos (Sentencia T-729/2002, 2002).

En la Sentencia T-787 de 2004 (2004), el Tribunal Constitucional señaló que es un derecho disponible, dado que ciertas personas, como se expresó en párrafos previos, pueden hacer públicas situaciones o conductas que otros preferirían mantener privadas. Adicionalmente, estableció que su núcleo esencial supone la existencia y goce de una esfera privada y reservada de cada individuo, permitiendo el pleno desarrollo de su vida personal, espiritual y cultural. Asimismo, dispuso que, aunque el hombre sea un ser social por naturaleza, no justifica que el Estado socialdemócrata, o la sociedad misma, pueda obligar a una persona a hacer público los ámbitos más íntimos de su vida personal. Por consiguiente, la existencia de la órbita privada e íntima de una persona estará exenta de la intervención del Estado y de la intrusión caprichosa de la sociedad.

La Corte, en la Sentencia C-640 de 2010 (2010), reiteró lo dispuesto en la Sentencia T-787 de 2004, donde recogió cinco principios que sustentan la protección del derecho a la intimidad. Los cuales se clasifican de la siguiente forma:

1. El principio de libertad dispone que los datos personales de un individuo solo podrán ser captados y divulgados bajo el consentimiento libre, previo, expreso o tácito del titular, salvo que el ordenamiento jurídico imponga la obligación de dar a conocer dicha información, con el objeto de cumplir con un fin constitucional legítimo.

2. El principio de finalidad indica que la captación y divulgación de los datos debe obedecer a una finalidad legítima, conforme a la Constitución, lo cual prohíbe obligar a los ciudadanos a revelar sus datos íntimos.

3. El principio de necesidad indica que la información personal que sea objeto de divulgación deberá tener relación con la finalidad pretendida, por lo tanto, está prohibida la divulgación de datos que desborden el fin constitucionalmente legítimo.

4. El principio de veracidad prohíbe que se divulguen datos que sean erróneos, equivocados o inexactos, por lo que deberán coincidir con la realidad aquellos que sean divulgados.

5. El principio de integridad, según el cual, la información objeto de divulgación deberá proporcionarse de manera completa, prohibiendo las divulgaciones parciales, incompletas o fraccionadas.

El conjunto de los principios enunciados permite garantizar la obtención legítima de la información personal, la objetividad en su divulgación y, en consecuencia, aseguran un debido proceso de comunicación. Por consiguiente, prescindir de ellos implicaría perder la intangibilidad del contenido garantista de la inmunidad del individuo frente a la innecesaria injerencia de los demás.

Años más tarde, la Corte distinguió tres maneras diferentes de vulnerar el núcleo esencial del derecho a la intimidad, recogidas en la Sentencia T- 407 de 2012 de la siguiente forma: la primera de ellas es la injerencia en la órbita reservada por cada persona; la segunda forma es la difusión de los hechos privados y, la tercera, es la exposición de aspectos personales de manera distorsionada o mentirosa (Sentencia T-407, 2012).

En este sentido, la injerencia o intromisión en la intimidad de la persona depende de cómo se ingresa a ese campo reservado, independientemente de lo que se publique; mientras que la segunda forma de vulnerar la intimidad, es justamente la divulgación de hechos privados sin tener previa autorización para ello. Por el contrario, la tercera manera de vulnerar la intimidad es la publicación o presentación errada o falsa de hechos íntimos, lo cual puede implicar a su vez la vulneración de derechos como la honra y el buen nombre (Sentencia T-696/1996, 1996).

Por otro lado, el Tribunal Constitucional recalcó en la Sentencia T-050 de 2016 los distintos niveles de intimidad: personal, familiar, social y gremial. El primero de ellos se refiere al derecho de una persona a estar sola y mantener sus aspectos íntimos bajo reserva; la segunda intimidad corresponde a la privacidad en el núcleo familiar, cuyo ejemplo es el derecho a la

inmunidad penal;[16] la tercera, alude a las relaciones de la persona en un entorno social delimitado, como los nexos laborales o vínculos interpersonales. Aunque el alcance de este derecho en dicho nivel es más reducido, se continúa protegiendo en aras de salvaguardar otros derechos constitucionales como la dignidad humana. Por último, el nivel de intimidad gremial hace referencia a las libertades económicas y la facultad de ocultar o abstenerse de explotar información, evidenciado, por ejemplo, en el derecho a la propiedad intelectual.

En términos generales, los grados de privacidad incluyen todo lo concerniente a la intimidad de las personas: relaciones familiares, costumbres, salud, prácticas sexuales, domicilio, comunicaciones privadas, *los espacios para la utilización de datos a nivel informático*, los secretos profesionales, creencias religiosas y toda información que cada uno revele de manera libre a los demás.

Finalmente, mediante la Sentencia C-094 de 2020, la Corte estudió la constitucionalidad de la Ley 1801 de 2016, Código Nacional de Policía, reiterando los principales lineamientos realizados por este órgano acerca del derecho a la intimidad, como los dispuestos en la Sentencia C-602 de 2016. En esta sostiene que dicho derecho le otorga al individuo la facultad de oponerse a: primero, la intrusión sin previa autorización en la órbita personal o familiar; segundo, la difusión de hechos privados y, tercero, la limitación a su libertad para tomar decisiones sobre asuntos personales. De igual manera, dicha providencia advirtió que el derecho a la intimidad acarrea, para las autoridades y particulares, el deber de abstenerse de efectuar hechos que supongan las acciones anteriormente mencionadas; y a su vez, impone el deber de tomar las medidas normativas, administrativas y judiciales necesarias para la protección de todas las dimensiones de este derecho (Sentencia C-602/2016, 2016).

Asimismo, indicó que el objeto de protección de este derecho es la vida privada y por ende, es fundamental definir lo que se entiende por público y privado, para conocer su alcance. Por tal motivo, el Tribunal ha señalado que la vida privada es un espacio, ámbito o esfera de los individuos, que abarca los espacios físicos, psicológicos y sociales de las personas.

Sin embargo, la Corte ha aclarado que el derecho a la intimidad no solo protege el espacio físico; no obstante, ha clasificado los espacios en: privados, semiprivados, semipúblicos y

[16] De acuerdo con este, "nadie podrá ser obligado a declarar contra sí mismo o contra su cónyuge, compañero permanente o parientes entro (sic) del cuarto grado de consaguinidad (sic), segundo de afinidad o primero civil" (Sentencia T-787/ 2004. 2004).

públicos. Se ha entendido como espacio privado aquel lugar donde las personas desarrollan su personalidad de manera libre en un entorno reservado, como la residencia y el domicilio.[17] Como lugares intermedios -entre el espacio privado y el público- la Corte ha definido que los espacios semiprivados son espacios cerrados cuyo acceso al público es restringido pero donde un grupo de personas participan de una actividad, como es el caso de colegios y oficinas de trabajo. A su vez, como otro espacio intermedio, ha establecido que los espacios semipúblicos son considerados como lugares de acceso parcialmente abierto a las personas que se sitúan en un momento determinado para realizar cierta actividad, como es el caso de cines y centros comerciales. Por último, en dicha Sentencia definió el espacio público como un lugar de uso común, en el que los individuos socializan, interactúan y se encuentran.

Se resalta la importancia de esta distinción, pues radica en que dependiendo del espacio visitado por el usuario, el nivel de satisfacción del derecho a la intimidad puede ser mayor o menor. Esto debido a que mientras más público sea el espacio, menor expectativa de privacidad habrá, pues las acciones afectarán y repercutirán más a otras personas en dichos espacios. Por tal motivo, aunque estos conceptos son definidos como "lugares", la vida privada se define como un espacio ontológico y no físico.[18] Así, se podría clasificar el Internet como un espacio entre lo público y lo semipúblico, en la medida en que es relativamente abierto[19] su acceso a las personas y allí comparten distintos intereses y situaciones.

Esto representa un reto frente a la regulación e implementación del uso de *cookies*. Es necesario definir el Internet en relación con una posible vulneración del derecho a la intimidad y no solamente el tipo de espacio en el que se encuentran los usuarios cuando navegan en Internet a través de los sitios *web*. También, se deben precisar dos cosas, primero, si la acción de quien alega la vulneración se encuentra protegida de la intromisión de otros y, segundo, si esa protección le era oponible a los que buscan manipular la información (Sentencia C-094/2020, 2020).

Como resultado de este recuento, se debe resaltar que, este derecho comporta la base de la protección de todo aquello que las personas no quieran dar a conocer de manera absoluta, ni

[17] Aunque para la Corte no se restringe únicamente a estos ejemplos, ya que comprende también los lugares de habitación, trabajo, estudio y todos los lugares en los que un individuo quiera desarrollar su vida sin la injerencia de terceros. (Sentencia C-094/2020, 2020).
[18] De conformidad con la Sentencia C-640 de 2010 (2010).
[19] A pesar de que la Corte no lo ha definido, es cuestionable el libre acceso al Internet por las barreras de conectividad, de estrato y sociales que existen en la sociedad, especialmente en Colombia.

siquiera cuando navegan en la *web*, ya que esperan un mínimo de confidencialidad y reserva frente a los datos que otorgan en Internet. Esto supone que, frente a herramientas como las *cookies* que rastrean el comportamiento en línea de un usuario, se requiera de igual forma el amparo de la intimidad. En otras palabras, los sitios y navegadores *web* deberán recopilar su información privada de manera legítima, es decir, contando con su autorización, y no podrán impedir la toma de decisiones frente a esta.

Por consiguiente, tal como lo señaló la Corte Constitucional desde el año 2001, a través de la Sentencia C-1147 (2001), en Internet la *intimidad* de los usuarios y el *habeas data* son dos derechos cuya naturaleza y características son diferentes. Estos entrañan el deber de asegurar garantías mínimas a todos los usuarios de Internet o a quienes desarrollan su emprendimiento por dicho medio. Lo anterior, se explica, ya que de una parte, el derecho a la intimidad supone que la información compartida en Internet está amparada por mecanismos de protección que buscan un grado de privacidad de los datos compartidos (según su naturaleza) y, de otra, en virtud del *habeas data*, se garantiza que dicha información no sea usada de forma inadecuada, debido a que se espera la recolección de datos precisos y necesarios para los fines de información e inspección requeridos.

3. RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES

En Colombia, el régimen de protección de datos personales se origina en el referido Artículo 15[20] de la Constitución Política de 1991. Es a partir de este precepto constitucional, que se expide la Ley 1266 de 2008 "Por la cual se dictan disposiciones generales del *habeas data* y se regula el manejo de la información contenida en bases de datos personales, de carácter financiero, crediticio, comercial, de servicios y la proveniente de terceros países" (p.1).

Sin embargo, a pesar de la existencia de dicha normativa, fue necesario expedir una ley que incorporara disposiciones generales sobre protección y tratamiento de datos personales. Por ende, cuatro años más tarde se promulga la Ley 1581 de 2012, que tiene como objeto desarrollar el derecho constitucional de *habeas data* y demás derechos, libertades y garantías establecidas en el Artículo 15 de la Constitución.

[20] Cuyo contenido y desarrollo jurisprudencial fue desarrollado en el anterior capítulo sobre Jurisprudencia de la Corte Constitucional.

Cabe agregar que, tanto la primera ley como la segunda han sido reglamentadas por diferentes decretos. La Ley 1266 de 2008, por el Decreto 1727 de 2009 y el Decreto 2952 de 2010. Y, por su parte, la Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013 y el Decreto 886 de 2014. Sin embargo, atendiendo a una de las finalidades que persigue la monografía, esto es, analizar el régimen normativo de datos personales a la luz del funcionamiento actual de las *cookies*, se procede a hacer un recuento de las disposiciones consagradas en la Ley 1581 de 2012 y el Decreto 1377 de 2013, debido a que regulan las generalidades sobre los datos personales.

3.1. LEY 1581 DE 2012

Aunque nos hemos remitido en varias oportunidades a esta Ley, es necesario dedicar un capítulo de la monografía para exponer su contenido y posteriormente en la monografía poder determinar una de las siguientes posibilidades:[21] primero, si la ley es suficiente por sí sola para regular el tema de *cookies* de cara a la nueva era digital; segundo, si no es suficiente debido a que el fenómeno de digitalización es completamente distinto a lo regulado, y en consecuencia, se requiere una nueva regulación, puesto que la legislación deja por fuera herramientas como las *cookies*; tercero, si la regulación vigente es parcialmente insuficiente, pues no reglamenta herramientas informáticas como las *cookies* y, por consiguiente, se deben ajustar ciertas disposiciones de la Ley 1581 de 2012 y del Decreto 1377 de 2013.

Para exponer el contenido de la Ley, hay que partir de que su objeto es desarrollar el derecho constitucional de *habeas data* propio de todas las personas para conocer, actualizar y rectificar toda información recogida sobre ellas en bases de datos o archivos por un responsable o encargado. Dicha información, establece la norma en el Artículo 4, se debe recaudar respetando los siguientes principios:

a) **Principio de legalidad en materia de Tratamiento de datos:** atiende a que el Tratamiento regulado por la ley es una actividad controlada, sujeta a lo establecido en ella y a las demás disposiciones que la desarrollen.

[21] Se aclara que el análisis que se lleve a cabo en los Capítulos 3 y 4 constituirá la base para determinar la viabilidad de alguna de las posibilidades propuestas. Por lo tanto, dicha elección y su respectiva justificación se expondrá en el capítulo 5 de la presente monografía, para así, lograr el estudio del régimen normativo de datos personales a la luz del funcionamiento actual de las *cookies*.

b) **Principio de finalidad:** el Tratamiento debe cumplir con una finalidad legítima, conforme a la Constitución y la Ley, que debe ser informada al titular por el responsable y/o encargado.
c) **Principio de libertad:** el Tratamiento y divulgación de los datos personales solo puede hacerse previo al consentimiento expreso e informado del titular, o previo a un mandato legal o judicial.
d) **Principio de veracidad o calidad**: hace referencia a que la información tratada debe ser completa, veraz, exacta, comprobable y entendible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
e) **Principio de transparencia**: el titular de los datos personales tendrá derecho, en cualquier momento y sin restricciones, a obtener información acerca de los datos tratados por el responsable o encargado.
f) **Principio de acceso y circulación restringida**: el Tratamiento sólo podrán realizarlo las personas autorizadas por el titular o aquellas previstas en la presente Ley.
g) **Principio de seguridad:** el Tratamiento de datos se debe realizar conforme a las medidas técnicas, humanas y administrativas necesarias.
h) **Principio de confidencialidad:** las personas intervinientes en el Tratamiento de datos personales "y 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" (Ley 1581, 2012, p. 3).

Del mismo modo, la Ley 1581 de 2012 precisa diferentes definiciones en su artículo 3, que permiten comprender lo establecido en ella, indicando que se entenderá por:

> a) **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
>
> b) **Base de Datos:** Conjunto organizado de datos personales que sea objeto de Tratamiento.
>
> c) **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
>
> d) **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

e) **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

f) **Titular**: Persona natural cuyos datos personales sean objeto de Tratamiento.

g) **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Ley 1581, 2012, p.2).

Respecto a los tipos de datos personales, la Ley 1266 de 2008 y Ley 1581 de 2012 compilan cinco tipos de datos: públicos, privados, semiprivados, sensibles y de menores de edad. Estos últimos, exigen medidas de seguridad más estrictas, debido a su relevancia en la sociedad y a su afectación a la intimidad del titular.

Además, dispone un título específico sobre los derechos que puede ejercer el titular, entre ellos: conocer, actualizar y rectificar sus datos personales recogidos en bases de datos; ser informado sobre su uso; solicitar prueba de la autorización otorgada al responsable del tratamiento; acceder en forma gratuita a los datos captados y, además, presentar reclamos o consultas sobre el tratamiento ante el responsable y/o Encargado. [22]

Correlativo a lo anterior, establece los deberes de los responsables y encargados del tratamiento. Por responsable se entenderá aquella persona natural o jurídica que, por sí misma o en asocio con otros, decida sobre el tratamiento de los datos. Y por encargado, aquella persona natural o jurídica que, por sí misma o en asocio con otros, realice el tratamiento de los datos personales por cuenta del responsable. Tanto el primero como el segundo, deberán garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de *hábeas data*. Además, deberán cumplir con los siguientes deberes: primero, informar debidamente al titular sobre la finalidad de la recolección y sus derechos; segundo, solicitar y conservar en las condiciones previstas en la presente Ley, copia de la respectiva autorización otorgada por el titular; tercero, conservar la información bajo las condiciones de seguridad necesarias y, cuarto, informar acerca de los datos de los responsables y canales de atención para el ejercicio de sus derechos, entre otros (Ley 1581, 2012, p. 8).

[22] Esto quiere decir que el Titular puede ejercer su derecho de *habeas data* frente a todo aquel que realice el Tratamiento de sus datos personales.

Por último, se establecen las funciones de la autoridad de protección de datos, indicando que la Superintendencia de Industria y Comercio, será la entidad encargada de asegurar la correcta aplicación de los principios, derechos y garantías previstos en la Ley 1581 de 2012, y, correlativamente, tendrá la competencia para darle aplicación al régimen de infracciones relacionado con el tratamiento de datos personales.

Así las cosas, la recopilación de los apartados anteriores constituyen los aspectos más básicos de la Ley de Protección de Datos Personales, en los cuales se evidencia que no hace alusión en ningún artículo o parágrafo sobre el uso de *cookies*, a pesar de ser una herramienta que puede captar datos personales.

3.2. DECRETO 1377 DE 2013

El Presidente de la República de Colombia en ejercicio de sus atribuciones constitucionales, y en particular las previstas en el Artículo 189 numeral 11 de la Constitución Política, con el fin de facilitar la implementación y cumplimiento de la Ley 1581 de 2012, reglamentó ciertos aspectos relacionados con: la autorización del titular para el tratamiento de sus datos personales; las políticas de tratamiento de los responsables y encargados; el ejercicio de los derechos de los titulares de la información; las transferencias de datos personales, y la responsabilidad demostrada frente al tratamiento de estos datos.

En principio, el Decreto dispuso, como la Ley 1581 de 2012, una terminología para la comprensión de su articulado, definiendo los siguientes aspectos: dato público, dato sensible, transferencia, transmisión y aviso de privacidad. Sobre esta última definición, de relevancia para la presente monografía, el Decreto señala que el aviso de privacidad es:

> 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 las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales (Decreto 1377, 2013, p. 2).

Posteriormente, en el capítulo II, referente a la autorización del titular para el tratamiento de los datos personales, el Decreto prescribe que su recolección deberá limitarse solo a aquellos que sean pertinentes y adecuados para la finalidad estipulada. A su vez, puntualiza que el responsable deberá solicitar, a más tardar en el momento de la recolección, la autorización del titular para realizar el tratamiento. Esto podrá hacerse de manera escrita, oral o mediante conductas inequívocas que permitan concluir de forma razonable el otorgamiento de la autorización. Además, precisa que, en ningún caso el silencio podrá asimilarse a una conducta inequívoca.

Respecto a las Políticas de Tratamiento de datos personales y avisos de privacidad, el Decreto establece el contenido mínimo que deben informar al usuario. A su vez, hace la salvedad de que la Política deberá constar en un medio físico o electrónico, redactadas con un lenguaje claro y sencillo, siendo puestas a disposición de los titulares.

Del mismo modo, indica quiénes estarán legitimados para ejercer los derechos del titular de los datos personales, y los mecanismos con los cuales puede hacerlos valer ante el responsable y encargado. Por último, el capítulo V del mencionado Decreto señala las reglas aplicables en la transferencia y transmisión internacional de datos personales.

El análisis preliminar constituye un recuento de los fundamentos generales que regula el Decreto 1377 de 2013. Respecto a su articulado, será objeto de estudio posterior lo referente a la autorización del titular para el tratamiento de los datos personales. Esto, en la medida en que los agentes que recolectan dicha información, a través de las *cookies,* deben solicitar su consentimiento en caso de que capten datos personales.

4. LECCIONES DE LA LEGISLACIÓN EUROPEA

Debido a la inexistencia de normas jurídicas para regular las *cookies* en Colombia, se realizará un análisis de la legislación de la Unión Europea (UE) en materia de datos personales como fuente auxiliar. Lo anterior, debido a que se ha convertido en una regulación valiosa para el juez constitucional o para el órgano legislativo, a la hora de tomar una decisión respecto al contenido del derecho de *habeas data* y su aplicación en el mundo digital. Así lo expresó la Corte Constitucional en la Sentencia C-748 de 2011:

> Los lineamientos europeos traídos a colación, en concepto de la Sala, no solo son una excelente herramienta para lograr una protección más efectiva del derecho fundamental al *habeas data*, que es un propósito que se impuso claramente el Constituyente en el artículo 15, sino una guía que el Gobierno Nacional debe seguir para cumplir los retos de un mercado globalizado, en el cual el individuo cada vez más, va perdiendo espacios de libertad y autodeterminación (2011).

En ese orden de ideas, se realizará un breve recuento de la normatividad más relevante sobre el régimen de protección de datos personales de la UE. Lo anterior, con el fin de conocer su origen y explicar el fundamento de la normatividad vigente.

Desde 1995 hasta mayo de 2018, el instrumento jurídico más importante de la UE en materia de protección de datos fue la Directiva 95/46/CE del Parlamento Europeo y del Consejo, 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. Su objetivo era armonizar las leyes nacionales en materia de protección de datos personales, que previamente habían adoptado diferentes Estados miembros y, así, garantizar un alto nivel de amparo y circulación de datos personales entre los Estados. Sin embargo, debido a que la Directiva no es fuente de aplicación directa,[23] muchos de los países interpretaron sus disposiciones con base en cada legislación nacional y, en consecuencia, la discrecionalidad conllevó a que se adoptaran diferentes normas de protección de datos (Agencia de los Derechos Fundamentales de la Unión Europea, Consejo de Europa, Supervisor Europeo de Protección de Datos y Tribunal Europeo de Derechos Humanos, 2018, pp. 34-36).

Además de la dispersión normativa, la evolución tecnológica ocasionó que la Directiva redactada perdiera vigor a mediados de la década de los noventas. Por ende, se convirtió en una prioridad reformar o modernizar la legislación de la UE en materia de protección de datos personales. Así, se dio paso al Reglamento General de Protección de Datos (RGPD) en abril

[23] Es preciso anotar la diferencia existente entre un Reglamento y una Directiva. Mientras que los Reglamentos son legalmente vinculantes en todos los países que conforman la UE desde su entrada en vigor, las Directivas deben ser incorporadas o "transpuestas" a la legislación nacional de los Estados Miembros. Por lo tanto, mediante la Directiva, se les ordena alcanzar un resultado, pero estos tendrán la potestad de elegir cómo hacerlo.

de 2016. Sin embargo, alcanzar dicho objetivo tomó más de tres años de redacción y alrededor de cuatro años de negociación entre el Parlamento Europeo y el Consejo de la UE.

Tras su adopción, el Reglamento establecía un período de transición de dos años, contados desde el 24 de mayo de 2016 hasta el 25 de mayo de 2018, fecha en la que entró en vigor y, consecuentemente, momento en el cual se derogó la Directiva sobre protección de datos del 1995.

Por su parte, en el 2002 se expidió la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (conocida como Directiva *e-Privacy*). A su vez, en el mismo año, en el territorio español se expidió la Ley 34/2002 por la cual se regula los Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI), que pretendía incorporar al ordenamiento jurídico español la Directiva 2000/31/CE.

A pesar de los incontables avances legislativos en materia de datos personales, la tecnología sigue evolucionando, de modo que, desde el 10 de enero de 2017, se tramita en la Comisión Europea la nueva propuesta del reglamento europeo sobre la privacidad y las comunicaciones electrónicas, conocido como Reglamento *e-Privacy*. Este, sustituiría la actual Directiva 2002/58/CE y derogaría la Ley 34/2002 de Servicios de la Sociedad de la Información (LSSI). Del mismo modo, se busca que este reglamento complemente al RGPD, ya que ambos regulan el tema de protección de datos personales, el primero, enfocándose en el ámbito digital y, el segundo, ampara situaciones que van más allá de este.

En ese orden de ideas, se presentarán las normas de carácter general que consideramos tienen mayor relevancia frente al objeto de la presente monografía, entre ellas, la Directiva 58/2002, y el Reglamento General de Protección de Datos. Asimismo, se estudiará la Guía sobre el uso de *cookies* de la Agencia Española de Protección de Datos Personales (AEPD) de 2019, con el objeto de extraer de esta los aspectos que posiblemente deban ser considerados en Colombia para proteger los datos personales captados a través de las *cookies.*

4.1. DIRECTIVA 58/2002: DIRECTIVA *E-PRIVACY*

De conformidad con el Artículo 1, el objeto de la presente Directiva es garantizar la protección de las libertades y derechos fundamentales en lo relativo al derecho a la intimidad, frente al

tratamiento y circulación de datos personales en el sector de las comunicaciones electrónicas.[24] Esta norma se aplica a las actividades incluidas dentro del Tratado constitutivo de la Comunidad Europea y el Tratado de la Unión Europea. De esta manera, se excluyen las actividades relacionadas con la seguridad pública, defensa y seguridad del Estado, así como las actividades en materia penal.

A partir de esta Directiva, se originó el marco jurídico de la Unión Europea para utilizar las *cookies*, ya que, por primera vez, se determinó una disposición específica sobre herramientas de recopilación de datos invisibles. En este sentido, el considerando número 24 establece que los equipos terminales de los usuarios deben ser protegidos de los identificadores ocultos, programas espías y otros dispositivos que se instalen sin su conocimiento, los cuales pueden acceder a información oculta o rastrear su comportamiento en línea. Lo anterior, supone una afectación a su intimidad y, por lo tanto, solo podrán utilizarse dispositivos que cumplan fines legítimos y con previo conocimiento de los usuarios.

Un ejemplo de lo anterior se evidencia en el considerando número 25, señalando cómo las *cookies* o "chivato" cumplen un propósito legítimo, por ejemplo, cuando analicen la efectividad del diseño y publicidad de un sitio *web* y, cuando faciliten el suministro de servicios de la sociedad de la información (Directiva 58, 2002, p. 3). Sin embargo, dispone que es un requisito *sine quo non* informar de manera clara y precisa sobre el uso de estos dispositivos, solicitando su autorización o permitiendo a los usuarios impedir su instalación. Este considerando indica a su vez, que estos 3 requisitos deben ser fácilmente accesibles al usuario. Sin embargo, le es permitido al responsable del contenido del sitio *web*, supeditar su acceso a la aceptación de la *cookie* en caso de que esta cumpla con un propósito legítimo.

[24] Artículo sustituido por el Artículo 1 de la Directiva 2009/136/CE del Parlamento Europeo y del Consejo cuyo texto es el siguiente:

> En el marco de la Directiva 2002/21/CE (Directiva marco), la presente Directiva tiene por objeto el suministro de redes y servicios de comunicaciones electrónicas a los usuarios finales. La presente Directiva tiene por objeto garantizar la existencia de servicios de comunicaciones electrónicas disponibles al público, de buena calidad, en toda la Comunidad a través de una competencia y una libertad de elección reales, y tratar las circunstancias en que las necesidades de los usuarios finales no se vean atendidas de manera satisfactoria por el mercado. La Directiva incluye asimismo disposiciones relativas a determinados aspectos de los equipos terminales destinados a facilitar el acceso de usuarios finales con discapacidad (Directiva 136, 2009, p.11).

Por su parte, el numeral 3 del Artículo 5, referente a la confidencialidad de las comunicaciones,[25] reitera que los Estados miembros de la UE deberán velar por el uso de redes de comunicaciones electrónicas que almacenen información de un equipo terminal, cuando se le brinde información clara y completa al usuario sobre los fines del tratamiento de sus datos. Además de otorgar la posibilidad de que éste acepte o rechace el tratamiento llevado a cabo por el responsable, cumpliendo con los lineamientos establecidos en la Directiva vigente en ese entonces, Directiva 95/46/CE. No obstante, esta disposición:

> [...] no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado (Directiva 58, 2002, p. 8).

En este orden de ideas, la norma analizada constituye el precedente de la regulación actual de las *cookies*, donde la solicitud de la autorización continúa como un requisito previo e indispensable para realizar el tratamiento de datos personales, a partir de la implementación de *cookies* a los sitios *web*.

Sin embargo, esta Directiva ha sido criticada por autores como Ian King (2003) considerando varios motivos: el primero cuestiona la ambigüedad de la expresión "fines legítimos" utilizada en el considerando 24, pues puede dar lugar a diferentes interpretaciones de las que pueden sacar provecho, por ejemplo, los sitios *web* para instalar *cookies* o cualquier dispositivo de rastreo; el segundo motivo, señala la ausencia de exigencias expresas, por parte del usuario, acerca de la información previa que le facilite aceptar o no la entrada de la *cookie* a su computador; por lo que es probable que este aviso se incluya dentro de la política de privacidad

[25]De acuerdo con el Artículo 2 (5) de la *Directiva 2009/136/CE del Parlamento Europeo y del Consejo*, el apartado 3 del Artículo 5 de la *Directiva 58/2002* se sustituye por el siguiente texto:

> 3. Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario (Directiva 136, 2009, p. 20).

que, por lo general, las personas no leen y, tercero, refiere que muchos usuarios de la *web* continuarán navegando sin ser conscientes de la instalación, finalidad y la forma para rechazar las *cookies* en sus dispositivos. Por último, la aceptación de las *cookies* no debería ser condición para acceder al contenido de un sitio *web* (pp. 234- 235), ya que esto beneficia más el interés comercial y no la privacidad de los usuarios, contrariando la posibilidad brindada por la misma norma a los usuarios de rechazar el almacenamiento de las *cookies* en su computador, tal como lo indicó el Grupo de Trabajo del Artículo 29 (GT29) o en inglés *Article 29 Data Protection Working Party* (Art. 29WP)[26] en *Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive* (Article 29 Data Protection Working Party [Art. 29WP], 2006, p. 3).

Por lo tanto, debido a que esta regulación resultó insuficiente para abarcar los riesgos derivados del uso de *cookies* y demás herramientas de rastreo recolectoras de información privada, se requirió la expedición de normas posteriores. Lo anterior, con el fin de suplir los posibles vacíos de esta norma y regular dichos dispositivos.

4.2. REGLAMENTO 679/ 2016: REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

El RGPD tiene por objeto establecer las normas referentes a la protección de las personas físicas en lo relativo al tratamiento de los datos personales y su libre circulación. Esta norma, de conformidad con el Artículo 2.1, se aplica tanto al tratamiento automatizado de datos personales, como al no automatizado de aquellos datos contenidos en un fichero. De esta manera, se excluyeron de su aplicación algunas actividades como las no comprendidas en el Derecho de la Unión[27], las realizadas por una persona física en su ámbito personal, las realizadas por autoridades competentes relacionadas con la actividad penal y seguridad pública, entre otras, establecidas en el Artículo 2.2.

[26] El Grupo de Trabajo del Artículo 29, fue creado mediante el Artículo 29 de la Directiva 95/46/CE como un organismo consultivo e independiente de la Unión Europea, que emite opiniones, dictámenes y recomendaciones en materia de protección de datos y privacidad. Actualmente con la entrada en vigencia del Reglamento General de Protección de Datos fue sustituido por el Comité Europeo de Protección de Datos.

[27] El Derecho de la Unión es la legislación de la Unión Europea. Esta consta de Derecho primario y Derecho derivado. El primero se refiere a los tratados que constituyen las reglas fundamentales de toda actuación de la UE. El segundo, por su parte, hace referencia a los reglamentos, directivas y decisiones que determinan los principios y objetivos de los tratados (Unión Europea, 2019).

Por su parte, el Artículo 3 determina que el Reglamento se aplica al tratamiento de datos personales que realice un responsable o encargado establecido en la Unión Europea, independientemente que dicho tratamiento se realice o no en este territorio. Asimismo, se aplica al tratamiento realizado por un responsable o encargado sobre los datos personales de un residente de la UE, cuando se recopilen a través de una oferta de bienes y servicios en la UE y/o cuando se realice un control de su comportamiento en la Unión. Lo anterior corresponde a uno de los cambios más novedosos introducidos por esta norma, ya que tiene implementación extraterritorial y permite su aplicación al funcionamiento de herramientas de rastreo como las *cookies*.

Para comprender el contenido del RGPD es necesario tener presente algunas definiciones establecidas en su Artículo 4.[28] En este sentido, la norma dispone qué se entenderá por:

1) **Datos personales**: Aquella información sobre una persona física identificada o identificable (el interesado). La persona identificable será aquella que pueda determinarse directa o indirectamente a través de un identificador como lo son: El nombre, número de identificación, datos de localización, identificador en línea o elementos de su identidad física, fisiológica, genética, psíquica, económica, cultural o social (Reglamento 2016/679 [RGPD], 2016, p. 33).
2) **Elaboración de perfiles**: Toda forma de tratamiento automatizado de datos personales para evaluar aspectos personales de una persona física, con el fin de analizar o predecir aspectos sobre su productividad profesional, situación económica, salud, intereses y preferencias, comportamiento, ubicación y movimientos.
3) **Seudonimización**: Es el tratamiento de datos personales que impide su asociación a una persona física, salvo la utilización de información adicional.
4) **Fichero**: Conjunto estructurado de datos personales, accesibles de acuerdo con pautas determinadas.
5) **Responsable del tratamiento**: Persona física o jurídica que determina los fines y medios del tratamiento.
6) **Encargado del tratamiento**: Persona física o jurídica que trate datos personales por cuenta del responsable.

[28] Se describirán aquellas definiciones "innovadoras" y diferentes respecto a las del régimen de protección de datos de Colombia, esto es, la Ley 1581 de 2012 y el Decreto 1377 de 2013, con el fin de que el lector tenga un panorama amplio del RGPD y evidencie los contrastes en este aspecto.

7) **Destinatario**: Persona física o jurídica al que se le comuniquen datos personales. Sin embargo, no se considerarán destinatarios las autoridades públicas que reciban datos dentro de una investigación.
8) **Tercero**: Persona física o jurídica distinta del responsable y encargado del tratamiento y de las personas autorizadas para tratar los datos personales.
9) **Consentimiento del interesado**: Es la manifestación de voluntad libre, específica, informada e inequívoca a través de la cual el interesado acepta el tratamiento de sus datos personales. Dicha manifestación requiere plasmarse en una declaración o mediante una clara acción afirmativa.
10) **Violación de la seguridad de los datos personales**: Aquella que genera la destrucción, pérdida o alteración, de manera ilícita o accidental, de los datos personales trasmitidos o tratados sin previa autorización.
11) **Tratamiento transfronterizo**: Aquel tratamiento realizado en dos contextos distintos. El primero de ellos, en el contexto de las actividades de responsables o encargados que se encuentren establecidos en más de un Estado miembro. Por su parte, el segundo, es aquel realizado en el contexto de actividades, de responsable o encargado, que afectan a interesados en más de un Estado miembro de la UE.

Así, es importante destacar que el RGPD establece un consentimiento explícito para permitir una manifestación libre e informada de la voluntad del interesado, garantizando con ello que la persona sea consciente de lo que esto implica. Lo anterior, constituye además una obligación para los responsables y encargados, ya que deben ofrecer información transparente y de fácil acceso y comprensión, tal como lo determina el principio de transparencia dispuesto en el literal a numeral 1 del Artículo 5.

De este modo, el Artículo 5 consagra unos principios que pueden resumirse de la siguiente manera:

A. **Principio de licitud, lealtad y transparencia**: Los datos personales deben ser tratados de forma lícita, leal y transparente.
B. **Principio de limitación de finalidad**: Los datos requieren ser recopilados con fines específicos, explícitos y legítimos.
C. **Principio de minimización de datos**: Los datos personales deben ser adecuados, pertinentes y limitados a los fines declarados.

D. **Principio de exactitud**: Los datos personales requieren ser exactos y actualizados, garantizando la supresión o rectificación de aquellos inexactos.
E. **Principio de limitación del plazo de conservación**: Los datos personales precisan mantenerse de tal manera que permitan la identificación de los interesados. Esto, durante el tiempo necesario para el cumplimiento de las finalidades exigidas para la recolección, a menos de que se trate de fines de interés público, científico, estadístico o histórico.
F. **Principio de integridad y confidencialidad**: Los datos personales se deben tratar de tal forma que se garantice su seguridad, incluyendo la protección contra el tratamiento no autorizado o ilícito, su destrucción o daño accidental.
G. **Principio de responsabilidad proactiva**: El responsable del tratamiento está obligado a aplicar los anteriores principios y demostrarlo.

El Reglamento señala en su Artículo 6, las condiciones para que el tratamiento sea considerado lícito (RGPD, 2016), así:

a) Cuando el interesado haya dado su consentimiento para el tratamiento de sus datos personales.
b) Cuando se necesite para ejecutar un contrato en el que el interesado participa.
c) Cuando sea necesario para cumplir una obligación legal aplicable al responsable.
d) Cuando sea necesario para proteger intereses esenciales del interesado.
e) Cuando sea necesario para el cumplimiento del interés público o el ejercicio de poderes públicos que tenga el responsable.
f) Cuando sea necesario para satisfacer intereses legítimos del responsable o de un tercero, siempre que no prevalezca los del interesado (p. 36).

Es fundamental comprender que el RGPD se expidió con la finalidad de abarcar aquellas problemáticas y fenómenos no regulados hasta ese momento, en especial lo relacionado con las nuevas tecnologías y su incidencia en la privacidad de los ciudadanos (Rallo, 2012, p. 16). Esto, debido a que los europeos vieron la necesidad de unificar los lineamientos para garantizar la protección de los datos personales de los interesados. En este sentido, uno de los puntos más enfáticos es el consentimiento. Por tal motivo, en el Artículo 7 se indicaron como condiciones para este: Primero, el responsable deberá demostrar la autorización del tratamiento emitida por el interesado; segundo, demostrar que se presentó la solicitud de consentimiento de manera clara, accesible y utilizando un lenguaje sencillo diferenciado por

los demás asuntos consentidos por el interesado; tercero, el interesado tendrá derecho a retirar su consentimiento cuando quiera, sin afectar la licitud del tratamiento realizado previamente y deberá ser tan fácil de retirar como cuando se otorgó y, por último, para verificar el consentimiento libre, se tendrá presente si mediaba un contrato supeditado al tratamiento de datos personales que no requieren su uso.

En este sentido, el GT29 (2017), analizando las directrices sobre el consentimiento, ha sido enfático en la obligación de diferenciar los fines con los que el responsable realiza el tratamiento de los datos. Esto es, en el evento en que un tratamiento cumpla varios fines, el interesado deberá otorgar su consentimiento para cada uno de ellos (p. 11), con el fin de garantizar que la autorización sea específica, de conformidad con el considerando 32 y el artículo 4.11.

De igual forma, la autoridad europea ha indicado que el consentimiento "no puede obtenerse mediante la misma acción por la que el usuario acuerda un contrato o acepta los términos y condiciones generales de un servicio" (GT29, 2017, p. 18). En otras palabras, la aceptación total de los términos y condiciones de un *sitio web*, por ejemplo, no se considerará como el consentimiento para el uso de datos personales. Así como tampoco bastará con la continuación de la navegación, frente al tratamiento de datos en sitios *web*, para satisfacer este requisito.[29]

Asimismo, dispone en el Artículo 8 las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.[30] De este modo, establece que se considerará lícito el tratamiento de los datos personales cuando se trate de un niño mayor de 16 años. Para los menores de esta edad, será lícito cuando el consentimiento lo haya otorgado el titular de su patria potestad. Estas condiciones deberán ser demostradas por el responsable.

Por su parte, el Artículo 9 establece como categorías especiales de datos personales, en primer lugar, aquellos que exponen el origen étnico, racial, las opiniones políticas, convicciones religiosas o filosóficas, o la afiliación sindical; en segundo lugar, los datos genéticos, biométricos cuyo tratamiento busque identificar, de forma precisa, a una persona física y, en tercer lugar, los datos relativos a la salud, la vida sexual o la orientación sexual de una persona.

[29] Tal como se explicó en el apartado sobre el consentimiento en el Capítulo 3 sobre la legislación colombiana.

[30] De acuerdo con el Artículo 4.25 del RGPD, los servicios de la sociedad de la información se definen a partir del literal b del numeral 1 del Artículo 1 de la *Directiva 2015/1535* del Parlamento Europeo y del Consejo. Este dispone que es todo servicio prestado a distancia y por vía electrónica, a cambio de una remuneración (Directiva 2015/1535, 2015, p. 3).

Lo anterior, con el fin de prohibir su tratamiento, a menos de que concurra alguna de las causales dispuestas en el apartado 2 de dicho artículo.

En el Capítulo III se determinan los siguientes derechos del interesado:

1. **Derecho a la información:** De conformidad con los Artículos 12, 13 y 14, se tiene derecho a recibir información sobre el responsable, el tratamiento que se dará a sus datos personales, las finalidades, sus derechos y mecanismos para ejercerlos. Además, esta información debe ser escrita, de acceso fácil y gratuito y con un lenguaje claro.
2. **Derecho de acceso:** De acuerdo con el Artículo 15, obtener del responsable la confirmación sobre los datos tratados, sus fines, destinatarios, plazo de conservación, la existencia de decisiones automatizadas y perfilamiento, etcétera.
3. **Derecho de rectificación:** El Artículo 16 señala que es el derecho a que los datos sean actualizados y revisados con el fin de evitar o corregir su inexactitud.
4. **Derecho de supresión:** De acuerdo con el Artículo 17, es el derecho a suprimir los datos y su publicación, cuando se presente alguna de las situaciones dispuestas, como el retiro del consentimiento, la ilicitud del tratamiento, entre otras.
5. **Derecho de limitación:** Obtener del responsable la limitación del tratamiento de los datos, esto es, un bloqueo de la información cuando se cumpla alguna condición descrita en el Artículo 18.
6. **Derecho a la portabilidad de los datos:** Es la posibilidad de recibir del responsable los datos personales en un formato único de uso común para transmitirlos a otro responsable, tal como lo establece el Artículo 20.
7. **Derecho de oposición:** Es el derecho a oponerse al tratamiento de datos personales en el caso de tratarse de fines distintos a los queridos y conocidos por el interesado, como por ejemplo la mercadotecnia directa, de acuerdo con el Artículo 21.
8. **Derecho a no ser objeto de una decisión basada solamente en un tratamiento automatizado:** De conformidad con el Artículo 22, es el derecho a oponerse al tratamiento de datos automatizado, incluyendo la elaboración de perfiles, que afecte al interesado o le produzca efectos jurídicos.

Por otro lado, el Capítulo IV refiere al responsable y encargado del tratamiento. De este modo, la sección 1 establece sus obligaciones generales. Así, el responsable deberá aplicar las medidas técnicas para garantizar el cumplimiento del RGPD, como lo son el código de conducta establecido en el Artículo 40, las políticas de protección de datos, la

seudonimización, entre otros. Lo anterior, ya que, de conformidad con el Artículo 25, el responsable deberá aplicar estas medidas en virtud del principio de protección de datos desde el diseño, esto es, tanto desde el momento de la determinación de los medios como en el tratamiento mismo. Asimismo, en aplicación del principio de protección de datos por defecto, este agente garantizará el tratamiento únicamente de los datos necesarios para cumplir sus finalidades.

En cuanto al encargado, el Artículo 28 establece que deberá ofrecer garantías suficientes para que el tratamiento sea conforme a este Reglamento. Este se regirá por un contrato o acto jurídico que lo vincule respecto del responsable y determine el objeto, duración, naturaleza, finalidad, tipo de datos personales e interesados, obligaciones y derechos del responsable (RGPD, 2016, p. 49).

A su vez, el RGPD determina unas obligaciones conjuntas para el responsable y el encargado. Una de ellas, dispuesta en el Artículo 30, es el registro de las actividades del tratamiento, es decir, cada responsable y encargado requiere constancia de los fines del tratamiento, los interesados, destinatarios y, también, cuando aplique, las transferencias internacionales de datos personales, los plazos para suprimirlos y las descripciones de las medidas de seguridad adoptadas. Otra, según el Artículo 31, es el deber de cooperación con la autoridad de control cuando esta lo requiera. Además, deberán incluir en su tratamiento la seudonimización y cifrado de datos personales, la confidencialidad, integridad, un proceso de verificación sobre el cumplimiento de esta norma, esto es, cumplir con la disposición 32 sobre seguridad del tratamiento. De esta manera, conforme al Artículo 33, cuando ocurra una violación de la seguridad de los datos personales, deberán notificarlo a la autoridad de control competente, dentro de las 72 horas siguientes a la constancia de la ocurrencia del hecho. Igualmente, deberán comunicárselo al interesado, cuando esto suponga un alto riesgo para sus derechos y libertades.

Por otra parte, esta norma determina en el Artículo 40 que, tanto responsable como encargado, deberán adherirse a los códigos de conducta elaborados por los Estados miembros, las autoridades de control y el Comité Europeo de Protección de Datos, para la correcta aplicación del RGPD. A su vez, estos agentes podrán certificarse para demostrar el cumplimiento de esta norma, a través de sellos y marcas de protección de datos.

El Capítulo V regula las transferencias de datos personales a terceros países u organizaciones internacionales, cuyo principio general es el establecido por el Artículo 44. Este determina que solo se realizarán transferencias de datos personales a un tercer país u organización si el responsable y encargado del tratamiento cumplen con los requisitos establecidos en este capítulo. Uno de dichos requisitos es el dispuesto en el Artículo 45. Este refiere la necesidad de la Comisión Europea de garantizar un nivel de protección adecuado por parte de ese tercer país u organización, de conformidad con los elementos del apartado segundo. Otro de los supuestos para realizar esta actividad se refiere al ofrecimiento de garantías adecuadas, a cambio de que los interesados cuenten con derechos exigibles y acciones legales efectivas, tal como lo señala el Artículo 46.

Por su parte, el Capítulo VI determina que cada Estado miembro tendrá su autoridad de control,[31] para velar por la aplicación del RGPD, con el objetivo de proteger los derechos y libertades fundamentales de las personas, frente al tratamiento y circulación de sus datos personales en la Unión. Lo anterior incluye funciones investigativas (Artículo 57), sancionatorias (Artículo 59) y la obligación de elaborar un informe anual de sus actividades.

De igual modo, en la Sección 3 de este capítulo, se dispone la creación del Comité Europeo de Protección de Datos como órgano encargado de: primero, supervisar la correcta aplicación de esta norma, asesorar a la Comisión Europea en lo relativo a la protección de datos personales en la UE; segundo, emitir directrices, recomendaciones y buenas prácticas para cumplir la primera función descrita; tercero, acreditar los organismos de certificación y su revisión periódica; cuarto, facilitar dictámenes a la Comisión; quinto, promover la cooperación e intercambios bilaterales de información y buenas prácticas entre las autoridades de control y, por último, mantener un registro electrónico de las decisiones adoptadas por las autoridades de control, entre otras de conformidad con el Artículo 70.

Por lo anterior, debido a las múltiples funciones descritas anteriormente, este Comité:

> [...] aunque formalmente aparenta sólo sustituir el anterior Grupo de Trabajo previsto en el art. 29 de la Directiva 95/46 (art. 29 WP), adquiere una nueva muy relevante

[31] En el caso de España, la Agencia Española de Protección de Datos (AEPD) es la autoridad estatal de control encargada de velar por el cumplimiento de la normatividad sobre protección de datos.

> posición institucional a la vista de la profunda centralización europea que preside la nueva normativa europea de protección de datos (Rallo, 2012, p. 39).

Por otro lado, el Capítulo VIII indica los recursos, responsabilidades y sanciones derivadas de la infracción a este Reglamento. Así, los interesados tienen derecho a: presentar una reclamación ante la autoridad de control del Estado miembro donde reside, labora o donde ocurrió la infracción, de acuerdo con el Artículo 77; la tutela efectiva contra una decisión jurídicamente vinculante de esta autoridad de control, según el Artículo 78; la tutela judicial efectiva contra un responsable o encargado, conforme a este mismo artículo; dar mandato a una entidad o asociación sin ánimo de lucro que actúe en este ámbito, presentando la reclamación para buscar una indemnización, de conformidad con el Artículo 80 y, finalmente, recibir una indemnización por los daños y perjuicios sufridos, conforme al Artículo 82.

Una de las sanciones establecidas son las multas administrativas contempladas en el artículo 83 del presente Capítulo. Estas se impondrán conforme a las circunstancias de cada caso y serán de dos tipos. El primero referido a las infracciones cuya multa máxima sea de diez millones de euros (10.000.000 EUR), cuando se incumplan las siguientes obligaciones: primero, las del responsable y encargado dispuestas en los Artículos 8, 11, 25 a 39, 42 y 43; segundo, las de los organismos de certificación al tenor de los Artículos 42 y 43 y, tercero, las de la autoridad de control dispuestas en el Artículo 41(4). La segunda clase de infracción es cuya multa máxima sea de veinte millones de euros (20.000.000 EUR), cuando se incumplan: los principios para el tratamiento, incluyendo las condiciones del consentimiento; los derechos de los interesados; las transferencias de datos personales a un destinatario en un tercer país u organización internacional; obligaciones del Derecho de los Estados miembros y resoluciones o limitaciones del tratamiento por parte de la autoridad de control.

Ahora bien, los conceptos analizados anteriormente revisten de gran importancia para la regulación de las *cookies*, ya que, el RGPD al ser un instrumento normativo cuyo objetivo es establecer un marco general de protección de datos, determina aspectos como el expuesto en su considerando 30. Este señala que las *cookies*, así como otros identificadores en línea (*v. gr.* direcciones IP, etiquetas por radio frecuencia), pueden asociarse a una persona física, dejando huellas que, al mezclarse con otros datos recibidos por los servidores, pueden ser usados para elaborar perfiles e identificarlas (RGPD, 2016, p.7) . Lo anterior, implica que esta herramienta de rastreo capte datos personales.

En este sentido, los datos captados a través de las *cookies* pueden ser objeto de comercialización por parte de los agentes de datos o *data brokers*, luego de recopilar la información, con el fin de desarrollar perfiles y clasificar los intereses de las personas. De esta manera, la compra y venta de datos conlleva en muchas ocasiones, el perfilamiento, señalado por el RGPD (2016) como uno de los tres tipos de tratamiento que supone un alto riesgo para los derechos y libertades de las personas. Esto comprende, además, el tratamiento a gran escala de datos sensibles y la "observación sistemática a gran escala de una zona de acceso público" (RGPD, 2016, p. 53).

Así, de conformidad con el Artículo 35, el responsable deberá realizar una evaluación de impacto cuando opte por alguno de dichos tratamientos, lo cual implica el análisis de los elementos descritos en el numeral 7. Esto es, primero, la descripción sistemática de las operaciones y fines del tratamiento; segundo, la evaluación de su necesidad y proporcionalidad; tercero, la evaluación de los riesgos para los derechos y libertades de los interesados y, cuarto, las medidas previstas para afrontar dichos riesgos, incluyendo medidas de seguridad y mecanismos de protección.

Con el fin de comprender lo antecedente, es menester profundizar sobre la elaboración de perfiles, a efectos de establecer su relación con las *cookies* e incidencia en los datos personales de los interesados. En este sentido, dicha práctica, de acuerdo con el Artículo 4 del Reglamento, se caracteriza por ser una forma automatizada de tratamiento, que se lleva a cabo frente a datos personales y su objetivo es evaluar aquellos aspectos de una persona física. Esta actividad implica, por lo general,[32] un tratamiento automatizado o decisiones automatizadas, las cuales se toman a través de medios tecnológicos sin la intervención del ser humano (GT29, 2018, p. 8). En otras palabras, mediante algoritmos se toman decisiones a partir de los datos, tanto entregados por las personas, por ejemplo, a través de formularios, como los captados de ellas en las aplicaciones y los inferidos, por ejemplo, de un perfil existente de la persona. Sin embargo, la creación de perfiles supone un riesgo para los derechos de los titulares de los datos personales, ya que, frecuentemente, se basa más en datos inferidos por otros y no en los entregados por el interesado.

[32] Se debe destacar que las decisiones automatizadas pueden realizarse con o sin la elaboración de perfiles, y viceversa. Aunque dependiendo del uso de los datos personales, un proceso de estas decisiones puede convertirse en un proceso de perfilamiento, tal como lo dispone el GT29 en *Directrices sobre la toma de decisiones individuales automatizadas y la elaboración de perfiles a los efectos del Reglamento 2016/679* (2017).

Por otra parte, otro inconveniente que representa el *profiling* es relativo a la inconsciencia de las personas sobre la creación e implicaciones de un perfil, incluyendo la perpetuación de los prejuicios existentes y la limitación de las preferencias con base en predicciones inexactas (GT29, 2017, p. 6). Es decir, por ejemplo, en caso de que una persona quiera comprar en un sitio *web* productos distintos a los consultados o comprados anteriormente, es probable que este no le muestre artículos diferentes a lo que las *cookies* han captado. Lo anterior, debido a que "el uso de perfiles puede determinar incluso la información a la que vamos a tener acceso, limitando también nuestro derecho a recibir información veraz o siendo objeto de auténticas manipulaciones" (Garriga, 2017, p. 136).

En suma, teniendo en cuenta las complejidades derivadas del perfilamiento y tratamiento automatizado, realizado a partir de la información recolectada por las *cookies*, el RGPD ha enfatizado en el principio de transparencia, con el fin de informarle al interesado acerca de su funcionamiento y finalidades. Por lo tanto, desde el considerando 60 se dispone que el responsable facilitará al titular toda la información necesaria para garantizar un tratamiento leal y transparente y, de este modo, podrá decidir si rechaza dicha finalidad cuando acarree graves consecuencias. Lo anterior, supone que estos tratamientos producen efectos jurídicos y afectan significativamente a las personas, ya que conforme al GT29, como efectos jurídicos se encuentran la vulneración de derechos como la cancelación de un contrato, la admisión a un país o el acceso a un beneficio social (GT29, 2017, p. 23).

Asimismo, en las *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del* Reglamento *2016/679* del GT29 (2017) ha definido que, el tratamiento de datos afecta significativamente a una persona si sus efectos son suficientemente relevantes en su vida. En otros términos, la decisión automatizada requiere alguno de estos resultados: afectar de forma considerable su comportamiento o elecciones, repercutir en el interesado de manera prolongada o permanente, o, en el peor caso, discriminarlo (p. 24). Así, algunos ejemplos de estas decisiones son aquellas que impacten la situación financiera de una persona, como la cualificación para la asignación de un crédito o que afecten su ingreso a una universidad o a un empleo.

Finalmente, luego de conocer el contenido del Reglamento, es necesario destacar que, en primer lugar, es un pilar fundamental en la protección de datos personales en Europa, dada su condición general y vinculatoriedad; en segundo lugar, establece aspectos necesarios para el tratamiento y circulación de los datos personales, aplicables a cualquier forma de

recolección.[33] Esto implica que, aunque la norma únicamente refiere a las *cookies* en una ocasión, para su correcta utilización se requiere la aplicación de sus disposiciones, en especial lo relativo al consentimiento libre, específico, informado e inequívoco.

4.3 GUÍA SOBRE USO DE LAS *COOKIES* DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS PERSONALES

Con el objeto de incorporar al ordenamiento jurídico español la Directiva *2000/31/CE del Parlamento Europeo y del Consejo,* el Estado español, consagró el apartado segundo del Artículo 22 de la *Ley 34/2002*.[34] Dicho precepto legal, regula los derechos de los destinatarios de los servicios y, en especial, el mencionado apartado, dispone aquello relacionado con las obligaciones surgidas por los prestadores de servicios al utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales. Esta disposición establece que:

> 2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
>
> Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.
>
> Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario (Ley 34, 2002, p. 8).

Por lo tanto, para facilitar el cumplimiento de esta norma, del Reglamento *679/2016* y de la *Ley Orgánica 3/2018*, la Agencia Española de Protección de Datos (AEPD) publicó en el año

[33] Excluyendo los tratamientos dispuestos en el numeral 2 del Artículo 2 del RGPD.
[34] Esta regula los Servicios de la Sociedad de la Información y de Comercio Electrónico.

2013 la *Guía sobre el uso de las cookies*,[35] elaborada en colaboración con la industria de los medios digitales y las agencias de publicidad. En resumen, lo que pretende la Agencia a través de la Guía, es que las entidades que usan *cookies* u otros dispositivos para almacenar y recuperar datos de un equipo terminal, como *local shared objects o flash cookies, web beacons o bugs*, "reflexionen y adopten decisiones sobre la solución más adecuada a sus intereses y modelo de negocio" (AEPD, 2019, p. 7), más que ofrecer una solución general y uniforme para el cumplimiento de la ley, debido a la complejidad planteada por el uso de las *cookies.*

Por lo descrito anteriormente, pareciera que las obligaciones derivadas del Artículo 22 de la LSSI y normas análogas, aplicaran a todo dispositivo de almacenamiento. Sin embargo, la Guía establece unas excepciones al cumplimiento de estas obligaciones. Así, las *cookies* utilizadas para permitir la comunicación entre el equipo del usuario y la red, y las estrictamente necesarias para prestar un servicio solicitado por el usuario, no deberán informar sobre el uso ni obtener el consentimiento del usuario.

Prueba de lo anterior, la AEPD cita el *Dictamen 4/2012* del Grupo de Trabajo del Artículo 29, el cual interpretó: "para que una cookie pueda estar exenta del deber de consentimiento informado, su caducidad debe estar relacionada con su finalidad" (AEPD, 2019, p. 13). Por lo tanto, dispuso que entre las *cookies* exceptuadas estarían aquellas que tienen por finalidad:[36]

1. La entrada del usuario.
2. La autenticación o identificación de usuario (únicamente de sesión).
3. La seguridad del usuario, por ejemplo, para detectar datos erróneos.
4. La sesión de reproductor multimedia.
5. La sesión para equilibrar la carga.
6. Personalización de la interfaz de usuario.
7. Determinadas *cookies* de complemento (*plug-in*) para intercambiar contenidos sociales.

[35] Dicha Guía se actualizó en noviembre de 2019, debido a los cambios normativos y, con esta versión se realiza el análisis del presente capítulo. Cabe resaltar que en el mes de julio de 2020 se actualizó nuevamente, debido a las aclaraciones realizadas en mayo por el Comité Europeo de Protección de Datos en las Directrices 05/2020,sobre el consentimiento. Sin embargo, las nuevas pautas deberán implementarse a más tardar el 31 de octubre de 2020, ya que para su adaptación se otorgó un período transitorio de tres meses (Legal Today, 2020).

[36] Respecto a la finalidad, el Grupo de Trabajo en el *Dictamen 4/2012* indicó que es mucho más probable que se consideren como exceptuadas las *cookies* de sesión que las persistentes.

Por otra parte, la Guía presenta una clasificación de *cookies*, estableciendo que pueden estar incluidas en diversas categorías:

Categoría	**Tipo de *Cookies***
Según la entidad que las gestione	*Cookies* propias *Cookies* de terceros
Según su finalidad	*Cookies* técnicas *Cookies* de preferencias o personalización *Cookies* de análisis o medición *Cookies* de publicidad comportamental
Según el plazo de tiempo que permanecen activadas	*Cookies* de sesión *Cookies* persistentes

Tabla 1. Elaboración propia a partir de la Guía sobre el uso de las cookies de la AEPD

4.3.1. OBLIGACIONES DERIVADAS DEL APARTADO SEGUNDO DEL ARTÍCULO 22 DE LA LEY 34/2002 DISPUESTAS EN LA GUÍA SOBRE EL USO DE LAS *COOKIES*

Ahora bien, retomando las obligaciones derivadas del apartado segundo del Artículo 22, la Guía establece dos obligaciones que le conciernen al proveedor del servicio: La obligación de transparencia y de obtención del consentimiento.

4.3.1.1. OBLIGACIÓN DE TRANSPARENCIA

Respecto a la primera obligación, más conocida como "deber de información", la AEPD plantea dos preguntas como base para resolver los cuestionamientos cuando se presente la información ante el usuario relacionada con las *cookies*. Estas son: ¿qué información debe facilitarse? y ¿cómo debe mostrarse esta información? Para resolver el primer interrogante, la AEPD remite a lo establecido en la *Ley 34/2002*, en la que se exige que la información facilitada a los usuarios sea clara, completa y con arreglo a lo dispuesto en el RGPD. Además, establece el deber de indicar cuáles serán las finalidades del tratamiento de los datos y el uso

dado. Todo ello se deberá presentar al momento de solicitar el consentimiento del usuario, para contar con información suficiente acerca del uso de *cookies* y su aceptación.

Con base en lo anterior, la información referida será presentada al usuario a través de una política de *cookies* (segunda capa) que contenga: primero, la definición y función genérica de las *cookies*; información sobre el tipo de *cookies* utilizadas y su finalidad; segundo, identificación de quién usa las *cookies*; tercero, información sobre la forma de aceptar, denegar, revocar el consentimiento o eliminar las *cookies*; cuarto, información sobre las transferencias de datos a terceros países realizadas por el editor; quinto, período de conservación y, por último, el resto de información exigida por el Artículo 13 del RGPD que no se refiera de forma específica a las *cookies*, por ejemplo, los derechos de los interesados (AEDP, 2019, pp 15-17).

Por otro lado, para resolver el interrogante sobre ¿cómo debe mostrarse esta información?, la Guía subraya que se debe redactar en un lenguaje claro, sencillo, transparente y evitando una terminología técnica. Lo anterior, con el fin de que un usuario pueda, *grosso modo*, comprender la información básica sobre qué son las *cookies* y cómo funcionan.

Asimismo, precisa que la información debe ser de fácil acceso y sugiere su presentación por capas. Además, que sea de fácil acceso, implica que el usuario pueda encontrarla a simple vista. Para ello, la Guía brinda unas sugerencias sobre los lugares más accesibles en los que se puede ubicar el aviso de *cookies.*

Ahora, en lo atinente a la presentación por capas, la AEPD acude a las directrices sobre transparencia del Grupo de Trabajo del Artículo 29, donde recomiendan el uso de avisos de privacidad por niveles. Lo anterior, pretende evitar la fatiga informativa, sin perjuicio de que la totalidad de esta, se encuentre recogida en un solo documento al que se pueda acceder con facilidad. Así las cosas, este sistema sugiere mostrar la información básica en una primera capa,[37] por medio de un aviso de *cookies*, barra, panel o un *banner*[38] y, en la segunda capa, a través de una política de *cookies.*

[37] Es decir, aquella que se "abre" cuando se accede al sitio *web*.

[38] De acuerdo con la *Guía sobre el uso de las cookies*, un *banner* es aquel "anuncio con forma de rectángulo horizontal ubicado en la parte superior de las páginas web y que puede usar tecnología gif, animado, flash o jpeg" (AEPD, 2019, p.14).

En la primera capa, se deberá indicar: i) quién es el editor responsable del sitio *web*; ii) cuáles son las finalidades de las *cookies* que se utilizarán; iii) información sobre si las *cookies* son propias (es decir, del responsable del sitio *web*) o también de terceros asociados a él;[39] iv) información genérica sobre el tipo de datos que se van a recopilar; v) el modo en el que el usuario puede aceptar, configurar y rechazar la utilización de *cookies*[40] y, por último, vi) se debe presentar un enlace claramente visible dirigido a una segunda capa informativa que incluya información más detallada sobre las *cookies*, esta sería, la política de *cookie*s (AEPD, 2019, pp. 19-20).

4.3.1.2. OBTENCIÓN DEL CONSENTIMIENTO

Retomando el hilo conductor, la segunda obligación del prestador del servicio es la obtención del consentimiento por parte del destinatario del servicio o usuario. Este deberá adquirirse de forma libre e informada, a través de fórmulas expresas como haciendo clic en la casilla "consiento", "acepto", u otros términos similares, o, a través de una acción inequívoca ejecutada por el usuario que, en todo caso, es deber del responsable indicar cuáles acciones constituyen esta clase de aceptación, por ejemplo, "seguir navegando en el sitio *web".*

Sobre esta última forma de aceptación, la AEPD dispone que el consentimiento se otorgó válidamente cuando: primero, el aviso que notifica el uso de *cookies*, se ubica en un lugar visible, de modo que su color, leyenda y tamaño aseguren que no pasará desapercibido por el usuario. Y, segundo, que el usuario realice una acción calificada como afirmativa, por ejemplo:

> Navegar a una sección distinta del sitio *web* (que no sea la segunda capa informativa sobre *cookies* ni la política de privacidad), deslizar la barra de desplazamiento, cerrar el aviso de la primera capa o pulsar sobre algún contenido del servicio, sin que el mero hecho de permanecer visualizando la pantalla, mover el ratón o pulsar una tecla del teclado pueda considerarse una aceptación (AEPD, 2019, p. 21).

En últimas, si el gestor utiliza la modalidad de "seguir navegando" como forma de obtención del consentimiento, deberá, en todo caso, incluir un botón en el panel o *banner* para rechazar todas las *cookies*, pues requiere ser tan fácil dar el consentimiento como retirarlo.

---

[39] Es menester señalar que la identificación de los terceros no deberá realizarse en la primera capa.
[40] Se debe advertir, además, que si se realiza una determinada acción se entenderá que el usuario acepta el uso de las *cookies*.

Finalmente, la Guía propone diferentes mecanismos de obtención del consentimiento, e indica cómo deberá recabarse cuando el usuario sea menor de 14 años o cuando un editor presta servicios a través de diferentes páginas *web.* A pesar de que la obligación recaiga sobre la aceptación, dicha situación no obsta para que el usuario pueda negarse o impedir la instalación de estos dispositivos.

Por otro lado, aunque el apartado segundo del Artículo 22 no hace referencia a quién es el responsable de dar cumplimiento a las disposiciones derivadas de este precepto, la Guía plantea que aquellos sujetos que usen las *cookies*, bien sea el editor del sitio *web* que introduce *cookies* propias o el gestor de una *cookie* de tercero, deberán observar las obligaciones de información y consentimiento. Lo anterior, salvo cuando las *cookies* cumplan las finalidades exceptuadas, enumeradas en párrafos anteriores. Por lo tanto, todos los sitios *web* que capten datos de sus usuarios, y siempre que éstos no sean estrictamente necesarios para su funcionamiento, tienen la obligación de informar claramente sobre el tipo de *cookies* y la finalidad de su captación de datos, así como el deber de obtener el consentimiento de los usuarios para destinar sus datos a tal efecto.

Ahora bien, una vez aclarado cuáles son las obligaciones derivadas del uso de *cookies* ¿qué consecuencias jurídicas se pueden presentar ante su incumplimiento? Una muy evidente son las sanciones pecuniarias impuestas por la AEPD. En un primer caso, esta entidad impuso una multa por valor de 30.000 euros (la cual se redujo a 18.000 por haber reconocido su responsabilidad) a una empresa por haber instalado *cookies* en el equipo terminal de los usuarios sin su consentimiento. Además, por no ofrecer la posibilidad de negarse a su uso, ni brindar la posibilidad de retirar el consentimiento expresado (Fernández, 2019, p. 30).

Otra sanción reciente, es la impuesta a la compañía Twitter en el mes de junio de 2020, en esta oportunidad, la Agencia indicó que:

> En el presente caso, si se accede a la página *web* www.twitter.com, y sin haber realizado ningún otro tipo de acción se ha comprobado que se instalan *cookies* no necesarias. Además, el mensaje que se edita para advertir sobre las *cookies* solamente indica que "si se sigue navegando se aceptan la utilización de *cookies*" pero no se da información de cómo rechazar las *cookies* o cómo gestionarlas de forma granular.
>
> Si existe un enlace en la parte inferior de la página con el título de "*cookies*", a través del cual se accede a la política de *cookies* (segunda capa), pero tampoco en esta capa

> se posibilita la acción de rechazar las *cookies* o de hacerlo de forma granular. La página se limita a informar como configurar los diferentes navegadores para la gestión de las *cookies* (AEPD, 2020, p. 5).

Con fundamento en las anteriores consideraciones, para dar cumplimiento a las obligaciones derivadas del Artículo 22 apartado segundo de la LSSI, es indispensable garantizar los derechos a la protección de datos de los usuarios. Por lo tanto, aquellas entidades que manipulen *cookies* u otros dispositivos de almacenamiento, deberán cumplir con la obligación de información y consentimiento, salvo cuando su finalidad esté exceptuada de dichos deberes. Asimismo, es de suma importancia aplicar la Guía con independencia de que se recojan o no datos personales y, en caso de que la respuesta sea positiva, deberá aplicarse las normas de protección de datos personales y las obligaciones derivadas del RGPD (López-Lapuente, 2013).

4.3.2. ANÁLISIS DE SITIOS *WEB* ESPAÑOLES A PARTIR DE LA *GUÍA SOBRE USO DE LAS COOKIES* DE LA AGENCIA ESPAÑOLA DE DATOS PERSONALES

En este capítulo se pretende exponer el panorama actual de cómo los sitios *web* españoles están cumpliendo el deber de información y consentimiento derivados del Artículo 22 apartado segundo de la *Ley 34/2002*. En razón de lo anterior, se emplearán las consideraciones realizadas por la AEPD en la *Guía sobre uso de cookies* (2019) en cuanto a la forma como se debe presentar dicha información al usuario (por capas) y cómo obtener su consentimiento respectivamente.

En ese orden de ideas, se analizarán los siguientes sitios: El Corte Inglés (Grupo empresarial de distribución de moda y belleza, tecnología, hogar, supermercado, entre otros productos y servicios), cuyo nombre de dominio se identifica con https://www.elcorteingles.es/; El Mundo, (Diario online líder de información en español), con URL https://www.elmundo.es/ y, por último, Iberdrola, (Compañía dedicada a la producción, comercialización y distribución de energía), con dominio https://www.iberdrola.es/.

Se tomará como muestra las tres compañías nombradas, ya que sus productos y servicios difieren uno de otro, permitiendo tener un espectro más amplio sobre cómo estas compañías,

con diversidad de actividades económicas, cumplen o no los requisitos establecidos en el Artículo 22 de la Ley 34/2002.

4.3.2.1. EL CORTE INGLÉS

El sitio *web* en estudio, proporciona a los usuarios el siguiente *banner* o aviso de *cookies* (Figura 1), visualizado en la primera capa parte inferior del portal *web*.[41] Este contiene la información básica requerida para la sección, indicando primero, la finalidad de las *cookies*, segundo, la identificación sobre si son propias o de terceros, tercero, un enlace que remite a la política de *cookies*, dentro del cual se posibilita al usuario, a través de la sección "Configuración de *Cookies*", la administración y desactivación de las *cookies* y, por último, un botón para aceptarlas o modificarlas.

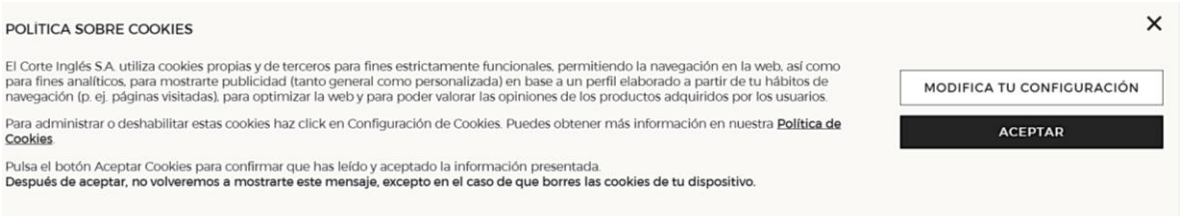

Figura 1. Información de la Política sobre *cookies* del sitio *web* El Corte Inglés.

En términos generales, El Corte Inglés observa las obligaciones derivadas del Artículo 22, proporcionando al usuario los estándares de información clara, completa y con un lenguaje sencillo. A su vez, en la Política de *cookies*[42] relacionan una figura (Figura 2) con las siguientes columnas (de izquierda a derecha): finalidad de cada una de las *cookies*, descripción de la *cookie*, nombre de la *cookie*, servidor de envío, propiedad (si son *cookies* propias o de terceros), si requiere o no consentimiento, fecha de caducidad y, por último, transferencia internacional. De esta manera, a nuestro criterio, facilita la toma de decisión del usuario para aceptar o rechazar las *cookies*, pues presentar la información detallada de los terceros que intervienen en la gestión de las *cookies*, la descripción, la posibilidad de elegir cuáles desea o no instalar en su

[41] Las imágenes que aparecen a continuación son extraídas de la página *web* El Corte Inglés cuya URL es https://www.elcorteingles.es/, para esta investigación.

[42] Es decir, la segunda capa cuya URL es https://cuenta.elcorteingles.es/politica-de-cookies/?modal=1%22#_ga=2.166473342.1963061404.1600907144-751533662.1600610969

dispositivo, entre otros factores, aseguran el consentimiento informado por parte del usuario y garantizan el cumplimiento de las obligaciones descritas en el capítulo antecedente.

Con base en lo anterior, consideramos relevante presentar un aparte de la figura señalada previamente (Figura 2), para facilitar la comprensión del lector, con el fin de visualizar la manera como se incorpora la normatividad al ámbito práctico en un sitio *web* español.

Personalización	Cookies de gestión para mejorar la experencia del usuario con los productos de la marca.	moulinex-companion	.elcorteingles.es	Propia	Sí	60 días	No
Analítica y optimización	Establece un valor anónimo para trazar las interacciones y patrones de navegación con el fin de mejorar la experiencia.	AWSALB	www.barilliance.net	Terceros	Sí	7 días	No
		__hssc	.hotjar.com	Terceros	Sí	365 días	No

Figura 2. Tabla con descripción de los aspectos de las *cookies* utilizadas por el sitio *web* El Corte Inglés.

En lo atinente al consentimiento y, con base en la información exhibida en el aviso de *cookies* (Figura 1) y política de *cookies*, todo parece indicar que las posibilidades en las que se pueden instalar las *cookies* son: Mediante la aceptación expresa del usuario a través del clic en el botón de "aceptar" o a través de las *cookies* exceptuadas del consentimiento. Adicionalmente, también expresan que al navegar y continuar en el sitio *web*, el usuario indica que autoriza el uso de las *cookies* y las condiciones dispuestas en la Política de *cookies*. Por otro lado, en cuanto a la forma de rechazar las *cookies*, la política remite a la configuración de los navegadores *web* para eliminar total o parcialmente el uso de estas.

A su vez, permite la modificación, por parte del usuario, de la configuración de las *cookies* (Figura 3). Esto es, la posibilidad de activar o desactivar las *cookies* que se almacenarán en su dispositivo, tal como se muestra en el siguiente *banner*:

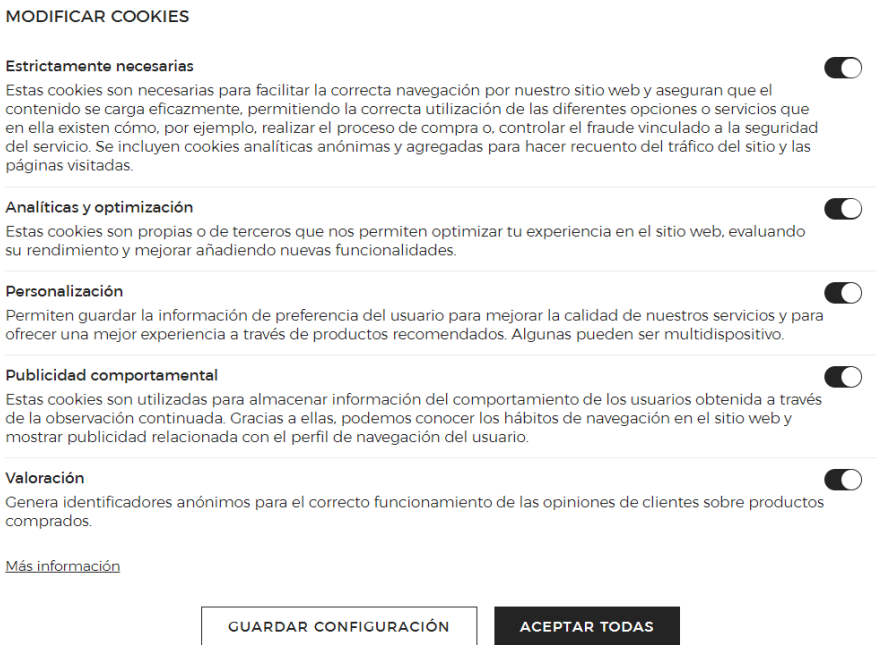

Figura 3. Descripción de las configuraciones para modificar las *cookies* en el sitio *web* El Corte Inglés.

Otro aspecto a resaltar es que el sitio *web* precisa en su política de *cookies* que dicha entidad no guarda datos personales de los usuarios a excepción de: La dirección IP, la información recogida para prestar un servicio solicitado por el usuario, como lo es la venta de los productos y servicios y, la posibilidad de recibir información sobre promociones y contenidos de su interés. Por lo tanto, como se expresó en párrafos anteriores, se deberá dar cumplimiento al Reglamento General de Protección de Datos Personales (2016).

4.3.2.2. EL MUNDO

Si bien son incontables las maneras de presentar la información derivada del Artículo 22 apartado segundo de la LSSI, el sitio *web* de El Mundo,[43] cumpliendo su obligación de transparencia, hace dos precisiones en su *banner* que merecen especial atención: primero, establece que su procesamiento se realiza sobre datos personales, cumpliendo con lo dispuesto en el RGPD. Y, segundo, estipula una finalidad más precisa[44] en cuanto al tratamiento de datos

[43] Las imágenes que aparecen en este apartado son extraídas de la página *web* El Mundo cuya URL es https://www.elmundo.es/, para esta investigación.
[44] A diferencia de los otros dos sitios *web* analizados, que indican que utilizarán *cookies* con el objetivo de prestar un mejor servicio y brindar una mejor experiencia de navegación.

a través de *cookies*. Lo anterior, permite al usuario una mayor seguridad jurídica respecto al uso de sus datos, en tanto cuenta con un marco más amplio para tomar una decisión informada.

Ahora, respecto al deber de información, el aviso de *cookies* (Figura 4) situado en la primera capa del sitio, se ubica en la parte superior de la *web*, lo que capta la atención del usuario y cumple con el fin de facilitar el acceso al contenido. Asimismo, se evidencian las finalidades, el uso de *cookies* propias y de terceros, y la remisión a la política de privacidad. Todo ello se plasma en el *banner* de la siguiente forma:

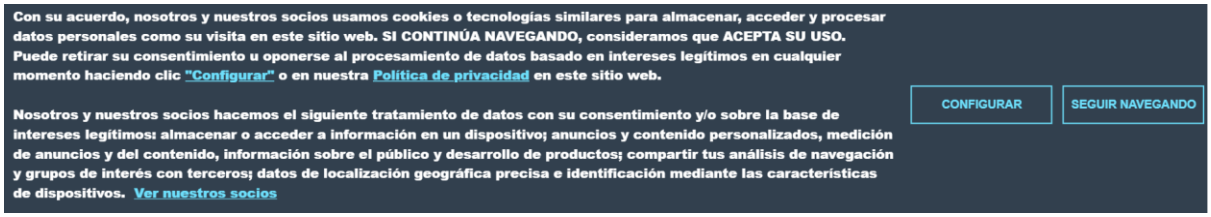

Figura 4. Descripción del aviso de *cookies* dispuesto en el sitio *web* El Mundo.

De este aviso se podría resaltar dos aspectos. El primero, es el vínculo de "Configurar", pues, al presionarlo, despliega automáticamente un aviso con un panel de configuración (Figura 5) para aceptar o rechazar cada una de las *cookies* clasificadas según su finalidad. Asimismo, haciendo clic en esta, se puede encontrar información adicional sobre su funcionamiento y uso. Esto se enmarca de la siguiente forma:

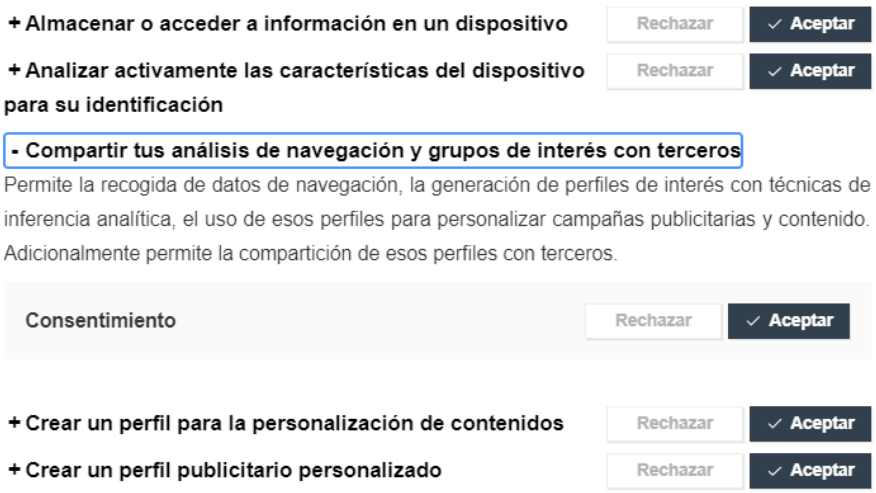

Figura 5. Configuración de las finalidades utilizadas por las *cookies* en el sitio *web* El Mundo.

El segundo aspecto, se enfoca en el listado de socios o terceros intervinientes en el uso de *cookies.* Así como la lista desplegable antecedente, el sitio dispone un panel similar al anterior (Figura 6). En este indican quién es el tercero, qué hace, qué datos recopila y cómo los usa. Esto permite al usuario consentir de manera independiente sobre el tratamiento realizado por los terceros gestores y, como lo denomina la Guía, presentar la información de manera granular.

Figura 6. Configuración de los terceros gestores de las *cookies* utilizadas por el sitio *web* El Mundo.

Por su parte, respecto al análisis de la política de *cookies*, es decir la segunda capa, el portal remite al sitio *web* de www.iabspain.net/privacidadeinternet/usuario para conocer información genérica sobre las *cookies.*

Respecto a los terceros, si bien la Política no determina quiénes son, el sitio sí facilita la opción de reconocerlos. Esto lo hace a través del panel previamente nombrado, seleccionando la opción de "Ver nuestros socios" en el *banner* situado en la primera capa. Adicionalmente, en la Política se establecen los tipos de *cookies* utilizados, y se enfocan en detallar cada uno de los propósitos de las *cookies* publicitarias y comportamentales. Por último, explican cómo desactivar las *cookies* analíticas, publicitarias y comportamentales, advirtiendo que su desactivación no afecta el funcionamiento del sitio *web.*[45]

Por otro lado, respecto al consentimiento, el sitio *web* implementa la aceptación expresa a través de dos opciones: Realizando la configuración individual de las *cookies* o mediante el botón de "Seguir navegando", que a diferencia de la primera, faculta al gestor de las *cookies*

[45] Lo cual difiere de lo dispuesto en el sitio *web* de El Corte Inglés, pues en este último, si se rechazan las *cookies* se afecta su funcionamiento.

a implementarlas en su totalidad. A fin de cuentas, en ambos casos, el usuario podrá tomar una decisión con base en información previamente entregada.

En últimas, el recuento previamente expuesto permite concluir que dicho sitio *web* cumple a cabalidad con el deber de información y consentimiento, pues brindan innumerables herramientas para tomar una decisión informada respecto al uso de *cookies*.

4.3.2.3. IBERDROLA

Del mismo modo que los sitios analizados, procedemos a exhibir el *banner* de *cookies* del sitio *web* de Iberdrola (Figura 7).[46] A diferencia de los anteriores, este aviso tiene dos particularidades: i) confiere la potestad al usuario de rechazar en primer plano el uso de *cookies* y, ii) no permite continuar navegando dentro del sitio *web* hasta que el usuario tome una decisión respecto al uso de estas, pues el *banner* lo sitúan en el centro de la pantalla sin ofrecer la opción de presionar el botón de *ESC.*

A pesar de la existencia de estas particularidades, que no son malas *per se*, el aviso situado en la primera capa, cumple con la mayoría de los estándares mínimos presentados por la AEPD en la *Guía sobre el uso de las cookies*. Esto, en tanto distingue las *cookies* que se instalarán en el dispositivo o navegador, además establece generalidades sobre su finalidad y el encargado de gestionarlas, la forma de rechazarlas y un vínculo que remite a la página *web* en donde se encuentra la política de *cookies.*

Figura 7. Aviso de *cookies* del sitio *web* Iberdrola. Recuperado de https://www.iberdrola.es/.

[46] Las imágenes que aparecen en este apartado son extraídas de la página *web* Iberdrola cuya URL es https://www.iberdrola.es/, para esta investigación.

Respecto a las obligaciones que estipula la Guía sobre cómo debe mostrarse la información, la política de *cookies* de Iberdrola, está redactada de manera clara y sencilla, indicando qué son las *cookies*, cómo funcionan, cómo se eliminan y cuáles son los tipos que utilizarán. Dentro de este último grupo, y, como se aprecia en el *banner* (Figura 7), se encuentran las *cookies* de terceros, a las que el responsable les otorga expresamente la obligación de información y consentimiento. Esto representa una ventaja para el usuario, pues conocerán quiénes serán esos terceros y bajo qué presupuestos harán uso de sus *cookies*. Por lo tanto, el sitio *web* presenta la siguiente figura (Figura 8) que permite cumplir con el deber de información, así:

FINALIDAD	TERCERO	MÁS INFORMACIÓN
Análisis: Son cookies estadísticas que nos permiten conocer datos útiles para mejorar nuestra página como, por ejemplo, medir la interacción de los usuarios con su sitio web permitiendo su seguimiento.	Google Twitter	Política de Google Política de Twitter
Publicidad: Son aquéllas que permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios de la página web, en base a criterios como el contenido editado o la frecuencia en la que se muestran los anuncios.	Doubleclick Facebook	Política de Doubleclick Política de Facebook

Figura 8. Descripción de las finalidades de las *cookies* utilizadas por terceros gestores en el sitio *web* Iberdrola.

Ahora, en lo atinente a la obligación de consentimiento, se utiliza la aceptación expresa como método de admisión a través del botón "Aceptar la política de *cookies*". En cuanto a la aceptación inequívoca, el sitio *web* no expresa nada sobre esta, por lo que se podría concluir que no utilizan esta forma. Cabe resaltar que la toma de esta decisión concerniente al usuario, se realiza con base en información previa y suficientemente clara para deliberar en cuanto al uso o rechazo de las *cookies.*

En resumen, en el análisis realizado, se puede determinar que los tres sitios *web* españoles cumplen con las obligaciones establecidas en el apartado segundo del Artículo 22 de la *Ley 34/2002* y con la *Guía sobre el uso de las cookies*. Esto se evidencia en la información aportada al usuario, su lenguaje, presentación y mecanismos para reconocer los terceros gestores, lo

que hace que la decisión que deba tomar sea informada y por ende, su consentimiento pueda estar basado en un contenido serio y que le genere seguridad jurídica.

4.3.2 ANÁLISIS DE SITIOS *WEB* COLOMBIANOS A PARTIR DE LA *GUÍA SOBRE USO DE LAS COOKIES* DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Si bien las compañías colombianas no están obligadas legalmente a presentar ante el usuario un *banner* y su respectiva política de *cookies*, es crucial evaluar la implementación que actualmente le dan los sitios *web* colombianos a estas. Por ende, debido a la inexistencia de una norma que regule este fenómeno dentro del territorio colombiano, se realizará el análisis con base en las obligaciones derivadas del Artículo 22 apartado segundo de la LSSI y, en consecuencia, se usará como referente lo estipulado en la *Guía sobre uso de las cookies* (en adelante la Guía) de la Agencia Española de Protección de Datos (AEPD) sobre la manera como se deben cumplir estas obligaciones. Se aclara, que dicha aplicación solo se realiza con fines académicos, puesto que no es aplicable directamente dentro del Estado colombiano.

En este sentido, los sitios *web* seleccionados como objeto de estudio son: Caracol Televisión S.A. (Compañía líder en televisión y radio), cuyo nombre de dominio es https://www.caracoltv.com/; Corona Industrial S.A.S., (Empresa dedicada a la manufactura y comercialización de productos para el hogar, la construcción, la industria, la agricultura y el sector de energía), con URL https://corona.co/ y, por último, Postobón S.A., (Sociedad especializada en la industria de las bebidas no alcohólicas en Colombia), cuyo dominio se identifica con https://www.postobon.com/. Se tomará como muestra las tres compañías nombradas, ya que, después de realizar un barrido en diferentes sitios *web* de empresas cuya representación en el mercado colombiano es relevante, se consideró viable estudiar aquellas que tuvieran diferentes maneras de informar sobre el uso de *cookies*. Lo anterior, permite contar con un espectro más amplio sobre cómo están dando a conocer la implementación de esta herramienta cuyo funcionamiento no está regulado por la ley.

En ese orden de ideas, tal como se estudió en el capítulo anterior, se expondrán los *banners* y políticas de *cookies*, es decir, la primera y segunda capa de los sitios *web*, con el fin de analizarlos de acuerdo con los parámetros establecidos previamente.

4.3.2.1. CARACOL TELEVISIÓN

Figura 9. Aviso de *cookies* dispuesto por el sitio *web* Caracol Televisión.

Este medio de comunicación, en su sitio *web*,[47] ofrece diferentes servicios para los usuarios, bien sea de información o recreación. Por lo tanto, cuando el usuario requiere satisfacer estas necesidades, el sitio mediante un *banner* le informa acerca de la posibilidad de utilizar *cookies* conforme a la política de *cookies*, a la que se puede acceder haciendo clic en "**haga uso de *Cookies* de acuerdo con esta Política**". Asimismo, establece dos posibilidades para obtener el consentimiento del usuario, esto es, la aceptación expresa por medio de un clic en "entendido", o por una acción inequívoca cuando se indica que se autoriza el uso de *cookies* si el usuario continúa la navegación.

De esta manera, se evidencia el cumplimiento de la obligación de obtener el consentimiento, pues se determinan las vías para ello, aunque se debe resaltar que la Guía es enfática en la necesidad de incluir un botón para rechazar todas las *cookies* cuando se utilice la acción inequívoca (AEPD, 2019, p. 21). Lo anterior, no se observa en la Política de *cookies*, pues la única manera dispuesta para rechazarlas es la configuración del navegador.

Respecto a la obligación de transparencia, se destaca que, dentro de esta primera capa se logra identificar: el editor responsable del sitio *web*, en este caso Caracol Televisión S.A., el modo de aceptación de las *cookies* y el enlace a la segunda capa correspondiente a la política de *cookies*. Esta define las funciones, tipos de *cookies* que se utilizarán, quién las implementará (tanto el editor como terceros) y cómo modificar la configuración del navegador para desactivar su uso.

En este sentido, pese a que la información se muestra de forma concisa, con un lenguaje claro y de fácil acceso, tal como lo expresa la Guía en el apartado 3.1.2, no cumple en su totalidad

[47] Las imágenes que aparecen en este apartado son extraídas de la página *web* Caracol Televisión S.A. cuya URL es https://www.caracoltv.com/, para esta investigación.

con los parámetros del apartado 3.1.2.2 sobre la información por capas. Lo anterior, dado que, en la primera capa no se determinan cuáles datos se recopilarán y, en la segunda capa, no se identifican quiénes son los terceros, cuáles son las consecuencias derivadas del perfilamiento y cuál es el período de conservación de las *cookies*.

En conclusión, Caracol Televisión cumpliría parcialmente con el apartado segundo del Artículo 22 de la LSSI, desarrollado por la Guía, ya que, a diferencia de los sitios *web* españoles, no es explícito en algunos aspectos fundamentales señalados frente a la transparencia. Esto, debido a que no toman en cuenta, por ejemplo, los efectos de la creación de perfiles con los datos personales del usuario.[48] No obstante, se destaca que el sitio *web* brinda información legible y previa al consentimiento e instalación de las *cookies*.

4.3.2.2. CORONA INDUSTRIAL

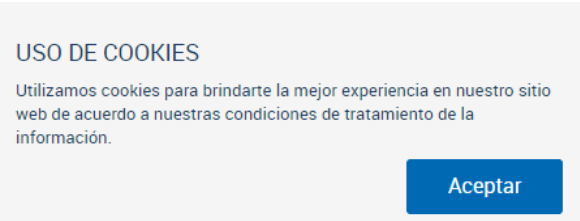

Figura 10. Aviso de *cookies* dispuesto en el sitio *web* Corona.

El segundo sitio *web* analizado es Corona, empresa antioqueña creada a finales del siglo XIX, cuyo objeto de mercado es la manufactura y comercialización de productos para el hogar. Al ser una empresa de gran reconocimiento económico en la nación, es relevante observar cuáles son sus políticas frente al objeto de estudio.

Al ingresar al sitio *web* de Corona Industrial,[49] en la parte inferior derecha se visualiza este *banner* con el aviso de *cookies* (Figura 10) que dispone del botón "Aceptar". Ahora bien, analizando esta primera capa, no se identifica específicamente su editor, pero se entiende que será Corona, de acuerdo con la política de tratamiento de Datos Personales, accesible a través

[48] Aquellos referenciados por el GT29, dispuestos en el apartado sobre el RGPD del Capítulo 4 de la presente monografía.
[49] Las imágenes que aparecen en este apartado son extraídas de la página *web* Corona Industrial S.A.S. cuya URL es https://corona.co/, para esta investigación.

de un hipervínculo.[50] A su vez, como se mencionó anteriormente, en el aviso de *cookies* se establece, de manera general, que estas se utilizarán con el fin de mejorar la experiencia de usuario, pero no se delimitan con precisión, por lo que se incumpliría lo dispuesto en la Guía. Asimismo, tampoco determinan si las *cookies* son propias o de terceros, ni el tipo de datos recopilados, ni el modo en el que el usuario puede configurar o rechazar las *cookies*, ni un enlace dirigido a una política de *cookies* como segunda capa.

Ya que el sitio *web* no cuenta con la capa mencionada, es necesario realizar la búsqueda en diferentes secciones o páginas *web* del sitio para expandir la información sobre las *cookies*. Así, en la sección de "Términos y Condiciones" se ubica un apartado denominado "Uso de *cookies*", en el cual detallan como finalidad, la recuperación de información sobre las preferencias y la sesión del usuario, para mejorar y personalizar su experiencia de compra. Igualmente, indica que el usuario podrá configurar su navegador de Internet para rechazar las *cookies.*

Sin embargo, esta información no se ajusta a los requisitos dispuestos en el apartado 3.1.1. sobre la obligación de transparencia de la Guía, por varios motivos. Primero, aunque es concisa, no se le brinda información suficiente acerca de qué son las *cookies*, sus finalidades, quién las utiliza (si el mismo editor o terceros), su período de conservación, cómo eliminarlas, ni si existe la posibilidad de elaborar algún perfil con los datos captados. Segundo, no utiliza un lenguaje claro y sencillo, pues emplea, precisamente, las expresiones que la Guía no considera válidas, esto es: "usamos *cookies* para personalizar su contenido y crear una mejor experiencia para usted" (AEPD, 2019, p. 18). Tercero, no es de fácil acceso, pues no hay un enlace que dirija directamente a este apartado, por lo que le corresponde al mismo usuario buscar la información al respecto. Lo anterior, contraría la obligación de separar la información sobre *cookies* de la información sobre términos y condiciones de uso o política de privacidad, tal como lo dispone la Guía.[51]

[50] Es decir, al dar clic en "Política de Tratamiento de Datos", se re direcciona a otra sección que contiene dicha Política en un archivo PDF, en la cual se establece que se aplicará tanto a Corona Industrial S.A.S. como a sus subordinadas en Colombia.

[51] En el apartado 3.1.2.3. se establece que: "A fin de mantener la visibilidad de la información sobre las cookies, esta deberá estar destacada y separada (mediante un hiperenlace distinto, por ejemplo) del resto de la información sobre términos y condiciones de uso o política privacidad" (AEPD, 2019, p. 22).

Por otro lado, se evidencia que este sitio *web* obtiene el consentimiento de los usuarios únicamente de manera directa a través del botón de "Aceptar", pues no menciona el uso de acciones inequívocas para ello. Sin embargo, el hecho de que la información acerca de esta herramienta sea confusa e incompleta, impide al usuario tomar una decisión libre, consciente y específica respecto a su autorización. No obstante, en caso de que el usuario acepte, no le será tan fácil retirar su consentimiento, ya que ni siquiera obtuvo asesoría frente a la configuración del navegador para rechazar las *cookies.*

4.3.2.3. POSTOBON

El último sitio *web* rastreado, corresponde a una empresa dedicada a la producción de bebidas con un gran trasegar frente a la economía colombiana.

En principio, el sitio *web* de Postobón, no evidencia un panel situado en la primera capa que alerte al usuario sobre el uso de *cookies.* Lo anterior conllevó a realizar una búsqueda por el sitio *web* con la finalidad de ubicar una posible sección referida a estas. Así, verificando la Política de Tratamiento de Datos Personales de la compañía, hallamos un apartado denominado "Respecto al uso de *cookies*".

En dicho apartado, el sitio *web* provee al usuario, mediante un lenguaje de fácil entendimiento, aspectos relacionados con el uso, tipo (analíticas, autenticación, sesión, y eventualmente *cookies* de personalización) y finalidad[52] de las *cookies*. Sin embargo, con relación a la claridad, llama la atención la siguiente expresión "no se recopilan datos personales como números de tarjetas de crédito u otra información de naturaleza financiera o crediticia" (Postobon S.A., 2015, p. 26). De este apartado podría entenderse: o que Postobón no va a recopilar los datos personales expresados taxativamente. o que captan datos personales pero diferentes a los enunciados, o que no capta ningún tipo de dato personal. Estos cuestionamientos ponen en duda la redacción planteada y, como consecuencia, generan confusión en el usuario, lo que podría nublar su decisión a la hora de consentir o no sobre el uso de *cookies.*

[52] Dentro de las finalidades, el sitio web señala que las cookies serán utilizadas para mejorar la experiencia en línea del usuario al conservar las preferencias previamente indicadas por él en las aplicaciones de La Compañía. Asimismo, establecen que otra de las finalidades es determinar cuántos usuarios visitaron las aplicaciones pertenecientes a este sitio.

Adicionalmente, en dicho apartado disponen dos temas relevantes. El primero, sobre la gestión de *cookies* de terceros que, si bien advierten sobre su uso, no señalan cuáles son los terceros a los que hacen referencia. Esta circunstancia diferencia a los sitios *web* españoles de los colombianos, pues los primeros discriminan uno a uno a los terceros intervinientes en el uso de estos dispositivos de almacenamiento. Y, el segundo, recae sobre el rechazo del uso de *cookies*, pues para hacerlo, se indica que muchos de los navegadores tienen la opción de rechazar nuevas *cookies* y desactivar las existentes, sin precisar cuál es el procedimiento para hacerlo o remitir a la página *web* de ese navegador que permite llevarlo a cabo.

Ahora bien, respecto a la obligación de consentimiento, si bien se cuenta con información bajo las precisiones descritas anteriormente, no se puede expresar dicha aceptación o rechazo de manera expresa debido a que no hay un *banner* que lo permita. Es decir, el usuario solo podría aceptar mediante una acción inequívoca como permanecer en el sitio, que, entre otras cosas, no está consagrada en el apartado de *cookies*, siendo otra circunstancia cuestionable para el usuario.

En ese orden de ideas, con la información planteada se podría tomar una decisión libre. Sin embargo, el contenido presentado no satisface muchos de los parámetros establecidos en la Guía, siendo esencial brindar información clara, completa, accesible y por capas, circunstancias que no se cumplen en su totalidad. Además, dicha inexactitud conlleva a que a la hora de tomar una decisión sobre el uso o no de *cookies*, el usuario no tenga el contenido suficiente para hacerlo.

En resumen, el análisis realizado anteriormente se puede presentar en la siguiente tabla:

Sitio *Web*	**Cuenta con aviso de *cookies***	**Cuenta con política de *cookies***
CARACOL TELEVISIÓN.	SI	SI
CORONA INDUSTRIAL	SI	NO
POSTOBON	NO	NO

Tabla 2. Elaboración propia

En conclusión, a partir del estudio realizado se evidenció que, pese a no existir una obligación para las compañías en Colombia de publicar un aviso de *cookies* y su respectiva política, es recomendable que le informen al usuario sobre el uso de esta herramienta, con el fin de garantizar el derecho de *habeas data*, teniendo en cuenta que es la facultad que tienen frente a su información. Esto, debido a que dichas herramientas de almacenamiento y rastreo, pueden captar datos personales para diferentes fines requeridos por un sitio *web*, por lo que es potestad del usuario aceptarlas o rechazarlas, en caso de que no consienta que sus datos sean objeto de tratamiento.

5. ALCANCE DEL RÉGIMEN DE PROTECCIÓN DE DATOS PERSONALES COLOMBIANO A LA LUZ DEL FUNCIONAMIENTO DE LAS *COOKIES*

El uso de Internet ha crecido de manera exponencial en los últimos años, convirtiendo el ciberespacio en un lugar alterno en el que confluyen diversos actores con una constante transmisión de datos. Estos últimos, adquieren relevancia, pues son indispensables para desarrollar diferentes ámbitos de la vida personal y, por consiguiente, es imprescindible la existencia de una regulación clara y eficaz sobre el tema. Lo anterior, con el fin de proteger efectivamente aquellos datos de naturaleza privada e íntima y, a su vez, permitir su acceso y tratamiento bajo determinadas condiciones.

Para llegar a este fin, en principio se necesita como fundamento el recuento llevado a cabo en capítulos anteriores. Esto es, los preceptos del régimen de protección de datos personales colombiano y, disposiciones del régimen europeo que sirven como complemento para visualizar el panorama actual del funcionamiento de las *cookies* y sus riesgos. Adicionalmente, se tomarán como base el texto denominado *Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital* de Newman y Ángel (2019) y algunos pronunciamientos del GT29. De esta manera, se centrará en el análisis de los aspectos que la legislación colombiana vigente no ha regulado y, aquellos efectivamente regulados, pero que requieren precisión.

5.1. ASPECTOS NO REGULADOS POR LA LEGISLACIÓN VIGENTE

En este apartado se abordará el estudio de los siguientes elementos: el uso de *cookies*, datos vinculados al Protocolo de Internet (IP), los contenidos personalizados, la comercialización de datos y las decisiones automatizadas. Esto, con el fin de identificar en qué consisten, su relación con los datos personales y, en consecuencia, su relación con las *cookies*. Para así, reconocer la necesidad de incorporarlos dentro de la normatividad colombiana y, con ello, garantizar la protección de los derechos al *habeas data* e intimidad de los titulares de los datos personales.

- **Uso de *cookies***

La Superintendencia de Industria y Comercio (SIC), autoridad encargada de garantizar que la recolección, uso, circulación y tratamiento de datos personales se realice conforme a la Constitución y la Ley, se ha pronunciado en múltiples oportunidades respecto a la protección de datos personales. Sin embargo, en relación con el uso de datos captados a través de las *cookies*, son dos los pronunciamientos de especial interés: el Concepto con radicado 16-172268 del nueve de agosto de 2016 y la Resolución número 12192 del primero de abril del 2020.

En el primero, la SIC a través de la Oficina Asesora Jurídica, reiteró el Concepto sobre datos personales y las características que ha precisado la jurisprudencia sobre estos. Entre estas se encuentran: "i) Estar referido a aspectos exclusivos y propios de una persona natural; ii) Permitir identificar a la persona en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos" (Sentencia C-748/2011, 2011). Al mismo tiempo, indicó que las *cookies* son archivos diseñados para captar información sobre los hábitos de navegación del usuario o de su equipo a partir del uso de una página *web*, además que, eventualmente, podrían conformar una base de datos. Por lo tanto, en este caso deberá aplicarse el régimen normativo de datos personales, conforme a las características jurisprudenciales indicadas con antelación. Asimismo, señaló que "en Colombia no existe una regulación específica sobre el uso de *cookies*" (SIC, 2016, p. 11).

En el segundo pronunciamiento, la SIC a través de la Delegatura para la Protección de Datos Personales, dio apertura a una investigación de oficio contra la compañía *Facebook Inc*. por fallas de seguridad en la plataforma. En la resolución expedida precisó que: "una cookie es un mecanismo que se instala en los equipos o dispositivos (bien sea celular, computador portátil,

u otro) de las personas residentes o domiciliadas en la República de Colombia con el objetivo de recolectar algunos de sus Datos". Además, agregó que: "las cookies son una herramienta para, entre otras, recolectar Datos personales" (SIC, 2020, p. 14).

Ahora bien, ¿por qué se destacan estos pronunciamientos? Se hizo énfasis en ellos, ya que permiten concluir tres aspectos fundamentales: primero, las *cookies* captan datos personales; segundo, no hay una normatividad específica que las regule y, tercero, aquel que manipule esta herramienta de recolección, al captar datos personales, se ceñirá a lo estipulado en la normatividad general sobre datos personales, es decir, la Ley 1581 de 2012 y normas que la reglamenten.

En efecto, no hay duda de que las *cookies* recolectan datos personales. Sin embargo, en nuestro sentir, la manera como lo hacen es diferente a lo expresado en la Ley 1581 de 2012. Esta ley describe la captación de los datos personales de la siguiente manera: por ejemplo, cuando un usuario se inscribe a un curso de un sitio *web,* debe diligenciar el formulario de inscripción ingresando sus datos personales y aceptando posteriormente el tratamiento de datos que lleve a cabo el sitio. Otro ejemplo, es cuando se debe introducir diferentes datos personales para crear una cuenta en un sitio *web* de empleo. Allí, el usuario voluntariamente inserta sus datos y acepta el tratamiento realizado sobre estos. En ambos casos, el titular es quien efectivamente está entregando sus datos para la recolección por parte del responsable y su manejo, con base en unas finalidades preestablecidas y conforme a la legislación vigente, garantizando la protección de su derecho de *habeas data* e intimidad.

Por el contrario, la manera como las *cookies* captan datos personales es diferente a la anterior. Tal como se explicó en el Capítulo 1.4., cuando un usuario accede a un sitio *web*, el servidor envía una respuesta *http* al navegador que contiene códigos como las *cookies*, las cuales, a su vez, contienen la información recolectada acerca de sus datos de navegación. Estos pueden incluir datos personales, preferencias, sexo, rango de edad, país de donde se conecta, intereses y en general, cualquier tipo de información que sirva para mostrar publicidad conforme a sus gustos. Sin embargo, es posible que el usuario no tenga conocimiento al respecto ni conozca cómo ejercer su derecho de *habeas data*, pues en muchas ocasiones no se le informa acerca del funcionamiento de esta herramienta.

Por lo tanto, si bien el concepto emitido por la Superintendencia remite a la normatividad general de datos personales, cuando se utilicen las *cookies* como herramienta de recolección,

consideramos que la regulación vigente es parcialmente insuficiente. Sin embargo, esto no quiere decir que se deba expedir una regulación particular, pues se podría ajustar la normatividad vigente acorde con la evolución tecnológica.

Prueba de lo anterior, en el Artículo 3 de la Ley 1581 de 2012, se dispone que la recolección de datos personales constituye una forma de tratamiento. Sin embargo, no establece criterios sobre las herramientas para llevarla a cabo. En esa medida, haciendo una aplicación al principio de legalidad, se deduce que estará permitido el uso de cualquier herramienta de recolección que no contraríe los preceptos establecidos en la Constitución y la Ley. En consecuencia, todo tipo de *cookies* podrá ser utilizada para realizar la recolección de datos, sin importar si son de sesión, propias, de terceros, permanentes, esenciales, personalizadas o para realizar análisis de los sitios *web*, debido a que no existe una prohibición expresa que se oponga a su implementación.

A pesar de lo anterior, consideramos que las *cookies,* al tener una relevancia tan significativa en el mundo digital, necesitan una reglamentación en el régimen de protección de datos personales. Aunque el uso de estas herramientas está permitido, los responsables de los sitios *web* no conocen sobre la información que deben brindar al titular de los datos, máxime cuando se haga uso de estas. Por ejemplo, es importante expresar qué tipos de *cookies* requieren del consentimiento previo del usuario, cuáles son sus finalidades, cómo rechazarlas y cuáles serían los efectos de ello, entre otras circunstancias.

Por ende, para resolver el inconveniente anterior, es necesario reestructurar los parámetros establecidos en el Decreto 1377 de 2013 sobre los contenidos mínimos de las políticas de tratamiento de datos personales y avisos de privacidad. En este sentido, bien sea para adicionar un artículo que reglamente las políticas de *cookies* o añadiendo un parágrafo dentro de los Artículos 13, 14 y 15, que disponga otros numerales en caso de que la política se refiera a *cookies.* A partir de estas premisas, todo aquello relacionado con los tipos de *cookies,* la finalidad de cada una de ellas, el proceso para desinstalarlas dependiendo del tipo de navegador, los terceros que depositan *cookies* en determinado sitio *web* y, las clases de *cookies* que estos utilizan, son factores relevantes que requieren disposiciones expresas en el régimen de protección de datos personales.

En conclusión, así como expresa la Superintendencia de Industria y Comercio citando a Maria del Carmen Guerrero, las *cookies* son herramientas “invisibles” que captan datos personales

(Guerrero, 2006, como se citó en SIC, 2020, p. 14). Por lo tanto, innegablemente la forma como lo hacen difiere de la señalada en la Ley 1581 de 2012. En consecuencia, es necesario ajustar dicha normatividad y, de ser el caso, se podría llegar a plantear además, la creación de una Guía o una Cartilla como las desarrolladas por la SIC[53] a partir del ajuste de la norma que haga más clara su aplicación. De esta manera, se garantiza una mayor seguridad jurídica para el titular (usuario), pues conocerá previamente acerca de estos archivos y, además, permite el ejercicio de su derecho de *habeas data* e intimidad, ya que se le brindarían herramientas para hacer uso de las facultades que estos derechos le otorgan.

- **Datos vinculados al Protocolo de Internet (IP):** Las siglas IP corresponden a *Internet Protocol* o en español Protocolo de Internet.

Este protocolo es el responsable de que la información pueda ser transmitida entre máquinas que están ubicadas en redes diferentes. En su acepción inicial, la expresión Internet se refiere a la interconexión de redes diferentes y, el protocolo, es el responsable de garantizar esta conexión.

La transmisión de información exige que se pueda identificar de manera única el emisor y el receptor de la comunicación. Para esto, la dirección IP, está conformada por una serie de números que siguen una estructura particular y permiten identificar un dispositivo en una red y establecer su conexión con esta. Un ejemplo de una dirección IP podría ser 187.23.202.151. Esta dirección tiene dos componentes: el identificador de la red y el identificador de la máquina. Cuando se envía un mensaje de una máquina a otra, se incluyen las direcciones IP del emisor y el receptor. Si las máquinas están en la misma red, la información se envía directamente del emisor al receptor utilizando el identificador de la máquina. Si están en redes diferentes, se utiliza la dirección de red para determinar cuál es la mejor ruta para llegar a la red de destino. Una vez el mensaje llegue a la red de destino, se utiliza el identificador de la máquina para hacer la entrega. La dirección IP se asigna a la máquina cuando se conecta a la red. Esta asignación puede ser estática, asignándole siempre la misma dirección, o dinámica, cuando cada vez es una nueva dirección. Los servidores normalmente tienen una dirección IP

[53] Por ejemplo, la Guía sobre tratamiento de datos personales para fines de marketing y publicidad (2019); Guía sobre el tratamiento de datos personales para fines de comercio electrónico (2019); Cartilla Ley 1266 de 2008 Habeas Data (2008).

estática, mientras que a las máquinas de usuario final, como portátiles o teléfonos celulares, por lo general, se les asigna una dirección dinámica o cambiante.

La dirección IP puede ser tanto pública como privada. La dirección pública es aquella que es única en todo el mundo y es visible en todo internet. Normalmente será asignada por el proveedor de la red. La dirección privada tiene la misma estructura que la pública, pero no es visible desde otras redes. Estas direcciones, a diferencia de las direcciones públicas, se pueden reutilizar libremente, permitiendo que haya muchas más máquinas conectadas a Internet.

Para utilizar direcciones privadas, es necesario que haya una máquina que tenga una dirección pública y una dirección privada, que sirve como puente entre la conexión a Internet y la red privada. Un ejemplo de dirección pública es la encontrada en el *modem* o *router* instalado en los hogares. Mientras que los dispositivos electrónicos conectados al *router* del hogar, ya sea impresora, celular, *tablet* o computador, tienen una dirección privada. Otro ejemplo es la conexión establecida dentro de la Universidad EAFIT. Esta se realiza a través de un *switch* que, a diferencia del *router* o *modem,* ofrece una mayor velocidad de conexión a los dispositivos conectados. En últimas, la dirección IP de la herramienta que conecta a Internet será pública, mientras que la dirección IP del dispositivo conectado será privada.

Así las cosas, la dirección privada es aquella designada a un dispositivo para ser reconocido dentro de una red local. Por lo tanto, el *router* o *switch* asignará esta dirección a los dispositivos conectados a su red y será el proveedor de servicios el encargado de concederla y el único facultado para conocerla. De tal forma que, los sitios y navegadores *web* no tendrán acceso a la IP privada de estos aparatos electrónicos.

Ahora bien, ¿por qué se hace referencia a esta dirección? La Ley 1581 de 2012 en el Artículo 3 literal c), establece que por dato personal se entenderá: “Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables” (Ley 1561, 2012, p. 2). Por ende, se plantea que la dirección IP, combinada con identificadores únicos y otros datos recibidos por los servidores, puede identificar, directa o indirectamente, la identidad de una persona determinable. Lo anterior, debido a que a través de la dirección IP se puede establecer la localización y características especiales del dispositivo, con capacidad de identificar a una persona. Un ejemplo de lo anterior se presenta cuando una persona busca artículos en un sitio *web* como el portal de Falabella. Allí el usuario, aún sin haber iniciado sesión y mediante la huella digital generada a través de las *cookies*, queda asociado con su IP.

En consecuencia, se podrá ofrecer un contenido personalizado, con base en sus anteriores búsquedas.

Newman Pont y Ángel Arango, citando al Grupo de Trabajo del Artículo 29 o *Article 29 Data Protection Working Party* (2000) señalan que:

> [...] los proveedores de acceso a Internet y los gerentes de redes de área local pueden, usando medios razonables, identificar a los usuarios de Internet a quienes les han atribuido direcciones IP, ya que normalmente "registran" sistemáticamente en un archivo la fecha, hora, duración y dirección IP dinámica entregada al usuario de Internet. Lo mismo puede decirse acerca de los proveedores de servicios de Internet que mantienen un libro de registro sobre el servidor HTTP [...] (Art. 29WP, 2019, p. 21 como se citó en Newman y Ángel, 2019, p. 50).

En efecto, se puede concluir que las direcciones IP permiten la identificación, de manera directa o indirecta, de una persona física. Por esto, la definición de dato personal dispuesta en la Ley 1581 de 2012 podría aplicarse, debido a que las características captadas por la IP permiten asociarla a una persona determinable.

A pesar de lo anterior, en nuestra opinión, aunque todas las herramientas tecnológicas desarrolladas no se pueden regular a través del derecho, es fundamental que la dirección IP, como un instrumento indispensable para el funcionamiento de un dispositivo, se pueda incluir dentro del concepto asociado al de dato personal. Así, como se evidencia en el Reglamento General de Protección de Datos Personales (2016) de la legislación europea, se entiende por dato personal:

> Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, **un identificador en línea** o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona[54] (p. 33).

[54] Negrilla propia.

- **Contenidos personalizados**

Uno de los propósitos para captar datos personales en los sitios *web* y, en general el de las compañías en Internet, es el ofrecimiento de contenidos personalizados. Esto es, contenidos ajustados a las preferencias y gustos de las personas, abarcando también anuncios y publicidad dirigida exclusivamente a ellas. No obstante, frente a este tema, el régimen de protección de datos personales colombiano solo establece la obligación de que esta finalidad se ajuste a la Constitución y la Ley. Además, que sea informada al titular cuando se recojan sus datos personales.

Así, en Colombia no se regula este asunto específicamente porque se omiten aspectos que ha resaltado el Grupo de trabajo del Artículo 29, en las Directrices *sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del* Reglamento *2016/679*, como los siguientes: i) para ofrecer publicidad personalizada se realiza un perfilamiento, o *profiling* en inglés, de los usuarios a partir de la información brindada. Esto quiere decir, que la persona entrega unos datos y la empresa que los recopila (en este caso el sitio *web*), a través de las *cookies*, por ejemplo, efectúa una serie de deducciones y conexiones, para fabricar una "nueva información" que el titular directamente no entregó. Por ello en Europa, por ejemplo, prescribieron la obligación de informarle esto posteriormente a la recolección de sus datos; ii) al crear perfiles se puede encasillar tanto a una persona, que puede discriminarse frente a los demás, al momento de ofrecer oportunidades laborales, créditos o seguros, por supuestamente no cumplir con el perfil adecuado para ello (GT29, 2017, p. 11). Además, es probable que estos perfiles no cuenten con una información suficiente sobre la persona y que estén incompletos o sean injustos en sus resultados.

Adicionalmente, hay otra particularidad que la normatividad sobre datos personales de Colombia no tiene en cuenta: la publicidad personalizada varía dependiendo del método que se utilice, tal como lo indica el GT29 en el *Dictamen 2/2010 sobre publicidad comportamental en línea* (2010). Lo anterior puede significar una mayor o menor invasión en la intimidad de las personas, ya que, por ejemplo, la publicidad comportamental, basada en la observación del comportamiento de las personas durante un período de tiempo, es el tipo de publicidad más invasiva. Para comprender esto, se necesita conocer lo que implica: en primer lugar, por lo general, la instalación de herramientas de seguimiento como las *cookies*, que rastrean la conducta del usuario, esto es, las visitas reiteradas a un mismo sitio *web*, interacciones en línea, etc; segundo, la creación de un perfil que puede ser "deductivo", como se describió

anteriormente, o "explícito", es decir, construido a partir de la información personal facilitada por el propio usuario luego de registrarse en un sitio *web* (Pérez, 2012, p. 15) y, por último, se basa en los intereses que el usuario demuestra en su navegación.

De este modo, el GT29 ha indicado en el referido Dictamen sobre publicidad comportamental (2010), que los usuarios, en términos generales, desconocen o no comprenden la tecnología que se utiliza para este tipo de publicidad, por lo que se requiere que el sitio *web* brinde información suficiente al respecto. Esto quiere decir, que se debe determinar la identidad del proveedor de la red de publicidad y el objetivo del tratamiento de los datos personales (GT29, 2010, pp. 19-20). Lo anteriormente expuesto, se justifica en la medida en que, mientras más información se obtenga sobre una persona en Internet, se podrá ejercer un mayor control sobre esta, ya que se puede influir en su comportamiento, deseos y decisiones.

Por último, otros temas no regulados específicamente por la legislación colombiana son la pluralidad de actores que intervienen en la mencionada publicidad y su dificultad a nivel tecnológico. Esto, dado que además de los editores *online* o *web publishers* (propietarios de los sitios y páginas *web* que comercializan espacios para publicidad), están los proveedores de redes publicitarias o *advertising network providers* (distribuidores de publicidad comportamental) y los anunciantes.

Así, los editores *online* conservan un espacio publicitario en su sitio *web* para que directamente los anunciantes, o por medio de los proveedores de redes publicitarias, puedan insertar la publicidad diseñada para los consumidores. Lo anterior se efectúa a través de las *cookies*, con el fin de monitorearlos, rastrear su comportamiento e identificar los perfiles coincidentes con los definidos por los actores enunciados previamente y, así, promocionar sus productos. En suma, ofrecer productos o servicios en Internet, utilizando publicidad comportamental, implica el uso de *cookies* y la participación de varios agentes que se aprovechan de los datos de los cibernautas sin su consentimiento. Por lo anterior, es necesaria una regulación expresa "para evitar tanto la invasión ilegítima de la privacidad de los usuarios/cliente" (Newman y Ángel, 2019, p. 66).

- **Comercialización de datos personales**

De conformidad con el principio de libertad dispuesto en la Ley 1581 de 2012, para realizar la compra y venta de datos personales en Colombia, se requiere el consentimiento previo, expreso e informado del titular o la existencia de un mandato legal o judicial que lo sustituya. Así, esta

actividad es legítima, tal como lo exige el principio de finalidad,[55] en la medida en que quien la realice esté facultado, ya que, de lo contrario, se configura el delito de violación de datos personales tipificado en el artículo 269F del Código Penal colombiano. Este penaliza las conductas referentes a la venta, compra u ofrecimiento de los datos personales contenidos en ficheros (*cookies*), archivos, bases de datos o medios semejantes, cuando no se esté facultado para ello, imponiendo penas privativas de la libertad y multas.[56] Sin embargo, dicha regulación incipiente no contempla los riesgos derivados de la compraventa de información, como el perfilamiento realizado por el *data broker* o vendedor de datos. Lo anterior, debido a que a través de esta práctica se puede ejercer un control social por parte de aquellos que ostentan el poder informático, tal como se señaló en el capítulo 2 de la presente monografía.[57] Riesgos que ha detectado el Grupo de Trabajo del Artículo 29, y que fueron explicados en el apartado 4.2. correspondiente al Reglamento General de Protección de Datos (RGPD).

En este sentido, las *cookies* actúan como dispositivos que recopilan datos personales, los cuales pueden ser objeto de comercialización y, con ello, a partir de un tratamiento indebido, puede vulnerar el derecho de *habeas data*. Esto, pues al transmitir ilimitadamente los datos de una persona sin su consentimiento, le impide tener un control sobre la información privada, que incluso hace parte de su intimidad.

- **Decisiones automatizadas:**

Estas resultan de la operación de una red de algoritmos sin la intervención del ser humano, que se explica en palabras de Sadin (2019): "la inteligencia artificial es capaz de manifestar autonomía decisional, es decir, tiene la capacidad de emprender acciones sin validación humana previa" (p.143). Dichas decisiones adquieren importancia en la medida en que condicionan aspectos como la publicidad *online*[58] y el perfilamiento; sin embargo, a pesar de

[55] Del literal b) del artículo 4 de la Ley 1581 de 2012.

[56] ART. 269F. - **Adicionado. L. 1273/2009, art. 1°. Violación de datos personales**. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (Código Penal Colombiano, 2000).

[57] En el Capítulo 2 se describió el poder informático y sus implicaciones en el *habeas data*.

[58] En este sentido, Reyes (2019) establece:

> Por ejemplo, una decisión automatizada sería la inclusión en determinados sitios web de anuncios sobre restaurantes de Valencia a usuarios que se conecten a dicha web desde una dirección IP13 ubicada en dicha ciudad. Esta inclusión de publicidad en línea, de forma automática, no implicaría la elaboración de un perfil del usuario residente en Valencia (ya que

la existencia y avance de la tecnología en este tema, no se ha regulado expresamente en Colombia, conllevando a que los únicos límites sean los principios dispuestos en la Ley 1581 de 2012 y el Decreto 1377 de 2013. En este sentido, la finalidad del tratamiento debe ser legítima conforme a la Constitución Política y la Ley y, a su vez, informada al titular.

No obstante, lo anterior no es suficiente para impedir el riesgo al que se someten las personas cuando aceptan un tratamiento que supone una decisión automatizada, pues en estos procesos se requiere que se "extremen al máximo las garantías legales y se adopten rigurosamente los principios de transparencia y consentimiento del interesado, así como que los procesos se diseñen desde el inicio de acuerdo con los principios de protección de datos personales" (Garriga, 2017, p. 138). En otras palabras, esta actividad implica para el titular

De este modo, es fundamental remitirse a la normatividad europea para comprender la importancia de regular este tema, ya que implica una serie de riesgos para los datos personales. Por lo tanto, dicha información fue ampliada en el capítulo 4.2, con base en el Reglamento General de Protección de Datos de la UE y los pronunciamientos del GT29. Estos suponen, que la toma de decisiones automatizadas adquiere mayor relevancia frente a los datos personales, captados a través de las *cookies*, en la medida en que sean utilizadas para elaborar perfiles de los usuarios. Lo anterior, debido a que esta práctica, como se evidenció anteriormente, conlleva a la vulneración del *habeas data*, pues los titulares no cuentan con la posibilidad de decidir sobre estos.

5.2. ASPECTOS REGULADOS QUE REQUIEREN PRECISIÓN

- **Consentimiento para llevar a cabo el tratamiento de datos personales**

Para analizar este ítem, se retomarán aspectos del capítulo segundo del Decreto 1377 de 2013, especialmente lo dispuesto en los Artículos 5 y 7. Estos regulan lo referente a la autorización para tratar datos personales y el modo de obtenerla respectivamente.

El Decreto señala que el responsable de realizar el tratamiento sobre los datos personales, deberá solicitar al momento de su recolección, la autorización del titular para ser tratados y, que a su vez, deberá informar sobre las finalidades específicas del tratamiento. En este sentido,

no se realizaría una evaluación sobre el usuario, simplemente se detectaría la dirección de IP conectada desde Valencia) (pp. 141-142).

para obtenerla, el Artículo 7 establece que se puede recabar por tres vías: "(i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la autorización", haciendo la advertencia de que "en ningún caso el silencio podrá asimilarse a una conducta inequívoca" (Decreto 1377, 2013, p. 3).

Esta última forma se ha implementado en mayor medida por los sitios *web*, disponiendo un aviso de *cookies* para indicar al usuario que al continuar navegando en el sitio (conducta inequívoca) está aceptando el uso de *cookies*. Por ende, implícitamente se está consintiendo sobre la captación, finalidades y tratamiento de datos personales consagrados en la política de *cookies*, en caso de que cuenten con ella.

En relación con ello, esta clase de aceptación presenta los siguientes riesgos: se está aceptando políticas de *cookies* no conocidas por los usuarios; son Políticas, que, debido a su extensión, un número reducido de usuarios suele leer; son Políticas que por su complejidad y vaguedad, pocas personas comprenden las implicaciones que conlleva aceptarlas y, coartan la libertad al titular de los datos personales de elegir los tratamientos y finalidades que desee autorizar, pues estos deben consentir sobre la totalidad de la información contenida en ella, sin tener la posibilidad de aceptar parcialmente esta política. En últimas, supeditan la prestación del servicio *web* a la aceptación total o en bloque de las *cookies.*

Lo anterior significa que, la aceptación inequívoca, entendida como aquella que "no admite duda o equivocación y permite concluir de forma razonable que el Titular otorgó la autorización para llevar a cabo el tratamiento de sus datos personales" (SIC, 2018, p.10), presenta un inconveniente significativo: saber si efectivamente la permanencia en el sitio *web* constituye o no una aceptación. En nuestra opinión, para resolver este interrogante, recurrimos a lo establecido por el Grupo de Trabajo del Artículo 29 en *Directrices sobre el consentimiento en el sentido del* Reglamento *(UE) 2016/679 (2017)*: "El silencio o la inactividad por parte del interesado, así como la simple permanencia de un usuario en un servicio no pueden considerarse una indicación activa de elección" (p. 18). Lo anterior, permite concluir que visualizar la pantalla, hacer *scroll* o realizar una mínima navegación, no podría considerarse una acción afirmativa de aceptación.

Asimismo, la forma como los gestores de las *cookies* están o no recabando el consentimiento conlleva a una posible vulneración de algunos principios consagrados en la Ley 1581 de 2012 y, a su vez, del derecho de *habeas data*. Así: i) los principios de legalidad y libertad, toda vez

que, cuando la información sobre una persona es recolectada sin contar con su consentimiento, se entenderá que fue adquirida de manera ilegal, pues la ley dispone que la aceptación para el tratamiento de los datos personales deberá realizarse de manera previa, expresa e informada; ii) el principio de finalidad, debido a que determinados sitios *web* no cuentan con un *banner* o política de *cookies* que informe al usuario, de manera previa, sobre el fin por el cual se recaudan sus datos personales, (iii) el principio de veracidad o calidad, pues, tal como se evidenció en el análisis realizado en el capítulo 4.3.3., el usuario no conoce con exactitud los datos que captan las *cookies* y, por ende, no tendría certeza si son veraces, exactos y actualizados, (iv) el principio de transparencia, ya que, en muchos sitios *web* no se evidencia la manera como el usuario (titular) puede ejercer su derecho de *habeas data*, es decir, no disponen de una ruta que brinde información acerca de los datos recopilados por las *cookies* y, (v) el principio de acceso y circulación restringida, dado que la persona desconoce, en muchas ocasiones, la existencia de terceros que instalan *cookies* y quiénes son, por lo que no estarían técnicamente autorizados.

A pesar de esto, el consentimiento no necesariamente debe ser solicitado por los sitios *web*. De esta forma, la Unión Europea dispone de unas excepciones razonables al consentimiento, permitiendo prescindir de la aceptación del usuario para captar datos a través de las *cookies.* Entre ellas se encuentran:

> [1] El uso de *cookies* esenciales, cuyo carácter "esencial" debe ser determinado desde el punto de vista del usuario más no del proveedor del servicio. Por ejemplo, una *cookie* de publicidad comportamental, podría considerarse como "esencial" desde el punto de vista del sitio *web*, pues es indispensable para su su estrategia de mercadeo. Sin embargo, no lo será desde el punto de vista del usuario. [2] *Cookies* estrictamente limitadas a propósitos estadísticos, donde la información deberá captarse de manera anónima. [3] Cuando las *cookies* sean necesarias para la transmisión de comunicaciones en la red de comunicaciones electrónicas. [4] La prestación de una funcionalidad explícitamente pedida por el usuario (Unión Europea, 2020).[59]

En ese orden de ideas, es necesario implementar políticas que presenten su contenido de manera precisa, concisa y comprensible para los usuarios. No se trata de qué tanta información se debe entregar al usuario, más bien, se trata de que esa información sea clara. Por otro lado,

[59] La información dispuesta en este apartado fue consultada el día 24 de agosto de 2020. Sin embargo, fue modificada el 14 de septiembre de 2020, por lo que para esta fecha el contenido citado ha variado.

la desprotección de los derechos de titulares de datos personales no puede excusarse en la creación de nuevas dinámicas tecnológicas. El fenómeno de la digitalización, y más el uso de *cookies*, se ha implementado hace más de 20 años y, actualmente, son indispensables para el funcionamiento de un sitio *web*. Por esto, se requiere un ajuste del régimen de protección de datos personales, que incluya este tipo de herramientas.

Es de suma importancia regular el tema, como se ha expresado en la jurisprudencia de la Corte Constitucional, a través de la Sentencia T-414 de 1992, que reza:

> Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en circulación perfiles de "personas virtuales" que afecten negativamente a sus titulares, vale decir, a las personas reales (Sentencia T-414/1992, 1992).

En efecto, lo anterior constituye un gran reto en materia de protección de datos personales, pues, con base en los aspectos señalados, se demuestra que el alcance de la regulación actual es insuficiente para atender las situaciones planteadas por el desarrollo tecnológico, en especial, las *cookies* como herramienta de recolección.

RECOMENDACIONES

A partir del recuento cronológico jurisprudencial de los derechos fundamentales de *habeas data* e intimidad y de acuerdo con las conductas realizadas por diferentes sitios *web,* se deduce que están potencialmente expuestos al riesgo de ser transgredidos debido al uso de *cookies*. Algunas de estas conductas son: la indebida notificación del uso de *cookies*, el uso sin consentimiento previo, la poca información brindada al usuario para la toma de una decisión, la inexactitud de los datos captados y la transferencia y/o comercialización de estos a terceros desconocidos por el titular. Dichas circunstancias generan, en muchas ocasiones, actos injustos, discriminatorios y manipuladores por parte de aquellos que ostentan el poder informático. En consecuencia, irrumpen en la autodeterminación informática del titular y, con ello, su potestad de decidir en qué momento y bajo qué límites da a conocer sus datos personales, es decir, se menoscaba el ejercicio del *habeas data*.

Por lo tanto, consideramos que para prevenir esta clase de riesgos, sería indispensable realizar un ajuste al régimen actual de protección de datos personales colombiano, mediante la incorporación de parágrafos o un articulado que se pronuncie respecto al uso de *cookies* y, análogamente, analizar la viabilidad de crear un documento similar a la *Guía sobre el uso de las cookies* de la Agencia Española de Protección de Datos Personales. De esta forma, se brinda mayor seguridad jurídica al cibernauta, en la medida en que existiría una norma expresa sobre el funcionamiento de estos archivos; y, a su vez, se impondrían mayores límites a las conductas realizadas por los gestores de los sitios *web*.

Dicho ajuste se debe realizar ya que, como se observó, la manera como los sitios españoles informan a las personas y obtienen su consentimiento para el uso de las *cookies*, es más apropiada y garantista en contraposición con la forma como lo hacen los sitios colombianos. En este sentido, los primeros exponen visiblemente un aviso de *cookies* en el que le explican al usuario su significado, uso, tipos y finalidades, con el fin de recabar su consentimiento; además de brindarles la posibilidad de aceptar o rechazar cada una de las *cookies* utilizadas y conocer quiénes serán los terceros implicados en el tratamiento. En contraste, no todos los sitios *web* colombianos analizados cuentan con aviso y/o política de *cookies*, tampoco indican de manera específica sus finalidades y tipos, ni la forma como se puede o no autorizar su implementación. Lo anterior, significa el desconocimiento del impacto que estos archivos tienen frente a los datos personales, *habeas data* e intimidad de los usuarios.

Algunos de los ajustes normativos que se requieren llevar a cabo en el régimen de protección de datos colombiano, son: primero, incluir el concepto de direcciones IP dentro de la noción de dato personal, pues al ser combinadas con otros datos permiten identificar al usuario. De esta manera, los sitios *web* estarían obligados a solicitar el consentimiento de los usuarios cuando recolecten información sobre su geolocalización, a través de las *cookies*. Segundo, imponer la obligación a los sitios *web* de solicitar la autorización del usuario cuando utilice *cookies* que capten sus datos personales,[60] con el fin de que sea previa, expresa y suficientemente informada, es decir, que pueda otorgarse conscientemente sin que haya lugar a equívocos. Por último, incorporar los tratamientos realizados con las finalidades de *profiling*, comercialización de datos y publicidad comportamental, para exigir su aceptación por parte del titular, garantizando los principios que rigen en el tratamiento de datos personales, e igualmente, los derechos de *habeas data* e intimidad.

Bajo este ideal, tanto responsables como encargados del tratamiento de los datos personales garantizarían una mayor protección de los derechos nombrados y, así, se evitarían posibles vulneraciones derivadas del tratamiento que ejercen al contenido captado por las *cookies.* Por consiguiente, los datos como: información sobre los hábitos de búsqueda y navegación, sitios visitados, ubicación, idioma, cuenta en línea y contraseña del usuario, tendrían una menor probabilidad de ser captados indebidamente y tratados bajo finalidades ilegítimas.

[60] Salvo cuando se utilicen *cookies* que estén dentro de las excepciones propuestas por el GT29.

REFERENCIAS

Agencia de los Derechos Fundamentales de la Unión Europea, Consejo de Europa, Supervisor Europeo de Protección de Datos y Tribunal Europeo de Derechos Humanos. (2018, abril). *Manual de legislación europea en materia de protección de datos*. Oficina de Publicaciones de la Unión Europea. doi:10.2811/824752

Agencia Española de Protección de Datos (AEPD). (2019). *Guía sobre el uso de las cookies*. https://www.aepd.es/sites/default/files/2019-12/guia-cookies_1.pdf

Agencia Española de Protección de Datos (AEPD). (2020). *Guía sobre el uso de las cookies*. https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf

Agencia Española de Protección de Datos (AEPD). (2020). Resolución de procedimiento sancionador PS/00299/2019. https://www.aepd.es/es/documento/ps-00299-2019.pdf

All about cookies.org. (S. f.). *¿Para qué se utilizan las cookies de sesión?*. Consultado el 03 de junio de 2020. https://www.allaboutcookies.org/es/galletas/cookies-de-sesion-utilizados-para.html

All about cookies.org. (S. f.). *¿Qué es un navegador?*. Consultado el 02 de abril de 2020. https://www.allaboutcookies.org/es/faqs/navegador.html

Article 29 Data Protection Working Party (Art. 29WP). (2000). Working document Privacy on the Internet - An integrated EU Approach to On-line Data Protection. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf

Article 29 Data Protection Working Party (Art. 29WP). (2006). Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp126_en.pdf

Bautista, M. (2015). El derecho a la intimidad y su disponibilidad pública. Universidad Católica de Colombia. https://repository.ucatolica.edu.co/bitstream/10983/14306/4/07_El-derecho-a-la-intimidad-y-su-disponibilidad-p%C3%BAblica.pdf

BBC Mundo. (29 de junio de 2017). *Qué ocurre cuando aceptas las cookies y por qué es conveniente borrarlas del navegador de vez en cuando*. BBC NEWS. https://www.bbc.com/mundo/noticias-40443519

Bloomberg. (15 de enero de 2020). Google lleva la publicidad digital a una nueva era sin cookies y las dejará de admitir por dos años. *La República*. https://www.larepublica.co/Internet-economy/google-lleva-la-publicidad-digital-a-una-nueva-era-sin-cookies-y-las-dejara-de-admitir-por-dos-anos-2952199

Caracol televisión. (s.f). [Gráfico]. Consultado el 11 de mayo de 2020. Recuperado de https://www.caracoltv.com/

Carmi, E. (2017). Regulating behaviours on the European Union Internet, the case of spam versus cookies. *International Review of Law, Computers & Technology*, 31(3), pp 302-303. doi: 10.1080/13600869.2017.1304616

Cervantes, F. (2009). Derecho a la intimidad y habeas data. *Derecho y Realidad*, (13), 27-35. https://revistas.uptc.edu.co/index.php/derecho_realidad/article/view/5010/4087

Código Penal Colombiano [CPC]. Ley 599 de 2000. Arts.269F. Julio 24 de 2000 (Colombia).

Constitución Política de Colombia [Const.]. (1991). Artículos 15,21,28,33,74,189 y 333. 20 de julio de 1991 (Colombia).

Corona. (2019). [Gráfico]. Consultado el 16 de mayo de 2020. Recuperado de https://corona.co/

Corte Constitucional (1992, 8 de mayo). Sentencia T-414/2019. (Ciro Angarita Baron, M.P.). https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

Corte Constitucional (1992, 22 de mayo). Sentencia T-011/1992. (Alejandro Martinez Caballero, M.P.). https://www.corteconstitucional.gov.co/relatoria/1992/T-011-92.htm#:~:text=T%2D011%2D92%20Corte%20Constitucional%20de%20Colombia&text=El%20art%C3%ADculo%20que%20consagra%20el,la%20dignidad%20de%20la%20persona

Corte Constitucional (1992, 16 de junio). Sentencia T-414/1992. (Ciro Angarita Baron, M. P.). https://bit.ly/3kQJqjX

Corte Constitucional (1992, 24 de junio). Sentencia T-425/1992. (Ciro Angarita Baron, M.P.). https://www.corteconstitucional.gov.co/relatoria/1992/T-425-92.htm

Corte Constitucional (1992, 18 de septiembre). Sentencia T-525/1992. (Ciro Angarita Baron, M.P.). https://www.corteconstitucional.gov.co/Relatoria/1992/T-525-92.htm

Corte Constitucional (1992, 7 de noviembre). Sentencia T-444/1992. (Alejandro Martinez Caballero, M.P.). https://www.corteconstitucional.gov.co/relatoria/1992/T-444-92.htm

Corte Constitucional (1993, 29 de enero). Sentencia T-022/1993. (Ciro Angarita Baron, M. P.). https://www.corteconstitucional.gov.co/relatoria/1993/t-022-93.htm

Corte Constitucional (1993, 3 de agosto). Sentencia T-303/93. (Hernando Herrera Vergara, M.P.). https://bit.ly/3l2EPLR

Corte Constitucional (1993, 25 de agosto). Sentencia T-340 /1993. (Carlos Gaviria Díaz, M.P.). https://www.corteconstitucional.gov.co/relatoria/1993/T-340-93.htm

Corte Constitucional (1995, 1 de marzo). Sentencia SU-082 de 1995. (Jorge Arango Mejía, M.P.). https://www.corteconstitucional.gov.co/relatoria/1995/su082-95.htm

Corte Constitucional (1995, 24 de abril). Sentencia T-176/1995. (Eduardo Cifuentes Muñoz, M.P.). https://www.corteconstitucional.gov.co/relatoria/1995/T-176-95.htm

Corte Constitucional (1996, 5 de diciembre). Sentencia T-696 /1996. (Fabio Moron Diaz, M.P.). https://www.corteconstitucional.gov.co/relatoria/1996/T-696-96.htm#:~:text=T%2D696%2D96%20Corte%20Constitucional%20de%20Colombia&text=La%20intimidad%2C%20el%20espacio%20exclusivo,sociabilidad%20natural%20del%20ser%20humano

Corte Constitucional (2000, 8 de mayo). Sentencia T-527/2000. (Fabio Moron Diaz, M.P.). https://www.corteconstitucional.gov.co/relatoria/2000/T-527-00.htm

Corte Constitucional (2001, 13 de junio). Sentencia C-616/2001. (Rodrigo Escobar Gil, M.P.). https://www.corteconstitucional.gov.co/relatoria/2001/c-616-01.htm

Corte Constitucional (2001, 31 de octubre). Sentencia C-1147 /2001. (Manuel José Cepeda Espinosa, M.P.). https://www.corteconstitucional.gov.co/relatoria/2001/C-1147-01.htm

Corte Constitucional (2002, de de septiembre). Sentencia T-729/2002.(Eduardo Montealegre Lynett, M.P.). https://www.corteconstitucional.gov.co/relatoria/2002/t-729-02.htm

Corte Constitucional (2004, 18 de agosto). Sentencia T-787 /2004. (Rodrigo Escobar Gil, M.P.). https://www.corteconstitucional.gov.co/relatoria/2004/t-787-04.htm

Corte Constitucional (2005, 23 de junio). Sentencia T- 657/2005. (Clara Inés Vargas Hernández, M.P.). https://www.corteconstitucional.gov.co/relatoria/2005/T-657-05.htm

Corte Constitucional (2008, 16 de octubre). Sentencia C-1011/2008. (Jaime Córdoba Triviño, M.P.). https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm

Corte Constitucional (2010, 18 de agosto). Sentencia T-640 /2010. (Mauricio González Cuervo, M.P.). https://www.corteconstitucional.gov.co/relatoria/2010/C-640-10.htm

Corte Constitucional (2011, 6 de octubre). Sentencia T-748/2011. (Jorge Ignacio Pretelt Chaljub, M.P.). https://bit.ly/30bAVrR

Corte Constitucional (2012, 31 de mayo. Sentencia T-407/2012. (Mauricio González Cuervo, M.P.). https://www.corteconstitucional.gov.co/relatoria/2012/T-407-12.HTM

Corte Constitucional (2016, 8 de febrero). Sentencia T-036/2016. (Gloria Stella Ortiz Delgado, M. P.). https://www.corteconstitucional.gov.co/relatoria/2016/t-036-16.htm

Corte Constitucional (2016, 10 de febrero). Sentencia T-050 /2016. (Gabriel Eduardo Mendoza Martelo, M.P.). https://www.corteconstitucional.gov.co/relatoria/2016/t-050-16.htm

Corte Constitucional (2016, 2 de noviembre). Sentencia C-602 /2016. (Alejandro Linares Cantillo, M.P.). https://www.corteconstitucional.gov.co/RELATORIA/2016/C-602-16.htm#:~:text=C%2D602%2D16%20Corte%20Constitucional%20de%20Colombia&t

ext=La%20Corte%20Constitucional%20encontr%C3%B3%20que,fundamental%20a%20la%20vida%20%C3%ADntima

Corte Constitucional (2018, 26 de junio). Sentencia T-238/2018. (Gloria Stella Ortiz Delgado, M. P.). https://www.corteconstitucional.gov.co/relatoria/2018/T-238-18.htm

Corte Constitucional (2019, 8 de mayo). Sentencia SU-182/2019. (Diana Fajardo Rivera, M.P.). https://www.corteconstitucional.gov.co/relatoria/2019/SU182-19.htm

Corte Constitucional (2020, 3 de marzo). Sentencia C-094 /2020. (Alejandro Linares Cantillo, M.P.). https://www.corteconstitucional.gov.co/relatoria/2020/C-094-20.htm

De Andrés, J., (2005). Glosario. En García, P. (Ed.), (2005). Principios de derecho de Internet. (pp. 600-602). Tirant Lo Blanch.

Decreto 1377 de 2013. [Ministerio de Comercio, Industria y Turismo]. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Junio 27 de 2013. D.O. No. 48.834. http://wsp.presidencia.gov.co/Normativa/Decretos/2013/Documents/JUNIO/27/DECRETO%201377%20DEL%2027%20DE%20JUNIO%20DE%202013.pdf

Digital Guide Ionos. (2018, septiembre 21). *Las cookies de terceros*. https://www.ionos.es/digitalguide/hosting/cuestiones-tecnicas/cookies-de-terceros/

Directiva 95/46/CE del Parlamento Europeo y del Consejo. 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. 24 de octubre de 1995. D.O. No. L 281 de 23/11/1995. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

Directiva 2002/58/CE del Parlamento Europeo y del Consejo. Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). 12 de julio de 2002. D.O. No. L 201 de 31/07/2002. https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_es.pdf

Directiva 2009/136/CE del Parlamento Europeo y del Consejo. Por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores. 25 de noviembre de 2009. D.O. No. L 337 de 18.12.2009. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:ES:PDF

Directiva 2015/15/35 del Parlamento Europeo y del Consejo. Por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (versión codificada). 9 de septiembre de 2015. D.O. No. 17.9.2015. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32015L1535&from=DA

El Corte Inglés. (s.f). [Gráfico]. Consultado el 24 de junio de 2020. Recuperado de https://www.elcorteingles.es/

El mundo. (s.f). [Gráfico]. Consultado el 5 de agosto de 2020. Recuperado de https://www.elmundo.es/

Expansión. (4 de septiembre de 2018). 10 cosas que no sabías de Google Chrome en su décimo aniversario. CNNEspañol. https://cnn.it/2ShkrKB

Fernández, C. (2019). La AEPD impone una sanción de 30.000 euros por no permitir a los usuarios de una web impedir la instalación de cookies. Revista Especial Directivos, 1764, 30-32.

Garriga, A. (2017). La elaboración de perfiles y su impacto en los derechos fundamentales. Una primera aproximación a su regulación en el Reglamento General de Protección de Datos de la Unión Europea. *DERECHOS Y LIBERTADES*, (38), pp 127-128. doi: 10.14679/1058

Grupo de Trabajo de Protección de Datos del Artículo 29 (GT29). (2010). *Dictamen 2/2010 sobre publicidad comportamental en línea.* https://studylib.es/doc/4697383/dictamen-2-2010

Grupo de Trabajo de Protección de Datos del Artículo 29 (GT29). (2012). *Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies*. https://www.apda.ad/sites/default/files/2018-10/wp194_es.pdf

Grupo de Trabajo de Protección de Datos del Artículo 29 (GT29). (2017). *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*. https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

Grupo de Trabajo del Artículo 29 sobre Protección de Datos. (2017). *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*. https://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp259rev01__es20180709.pdf

Guerrero Picó, María del Carmen. (2006). *El impacto de Internet en el Derecho Fundamental a la Protección de Datos de carácter personal*. Primera ed. Navarra: Thomson Civitas. p 25

Iberdrola. (s.f). [Gráfico]. Consultado el 13 de julio de 2020. Recuperado de https://www.iberdrola.es/.

Kemp, S. (2020). *Digital: 2020: Global Digital Yearbook [Digital 2020: Anuario global digital]*. We are social y Hootsuite. https://bit.ly/3kQrS7B

King, I. (2003). On-line privacy in Europe—new regulation for cookies. *Information & Communication Technology Law*, 12(3), 225-236. doi: 10.1080/1360083032000198745

Ley 34/2002. Ley de servicios de la sociedad de la información y de comercio electrónico. 11 de julio de 2002. BOE No. 166 de 12 de julio de 2002. https://www.boe.es/buscar/pdf/2002/BOE-A-2002-13758-consolidado.pdf

Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 18 de octubre de 2012. D.O. No. 48.587.

López-La Puente. (2013). El uso de cookies en España a la luz de la *Guía sobre el uso de las cookies* de la Agencia Española de Protección de Datos. *Actualidad Jurídica Uría Menéndez*, (35), 93-97. https://www.uria.com/documentos/publicaciones/3912/documento/fe3.pdf?id=4799

Legal Today (2020, julio 30). *La AEPD actualiza su Guía sobre el uso de cookies para adaptarla a las nuevas directrices del Comité Europeo de Protección de Datos*. https://www.legaltoday.com/actualidad-juridica/noticias-de-derecho/la-aepd-actualiza-su-guia-sobre-el-uso-de-cookies-para-adaptarla-a-las-nuevas-directrices-del-comite-europeo-de-proteccion-de-datos-2020-07-30/

Luján, S. (2011, octubre 30). *Cookies: ¿Qué son y para qué sirven?* [video]. YouTube. https://www.youtube.com/watch?time_continue=1&v=8LaTgXMhgtE&feature=emb_logo

Milenium. (S. f.). Sitios Web. Consultado el 02 de abril de 2020. https://bit.ly/2S1tP4P

Ministerio de Tecnologías de la información y las Comunicaciones (MinTIC). (2019). Boletín Trimestral de las TIC: Cifras Segundo Trimestre de 2019. https://colombiatic.mintic.gov.co/679/articles-106955_archivo_pdf.pdf

Newman, V. y Ángel, M. (2019). Rendición de cuentas de Google y otros negocios en Colombia: la protección de datos personales en la era digital. Dejusticia. https://cdn.dejusticia.org/wp-content/uploads/2019/01/Rendicio%CC%81n-de-cuentas-de-Google-y-otros-negocios-en-Colombia.pdf

Oró, R. (2015). La protección de datos. UOC

Pérez, F. (2012). La publicidad comportamental online. UOC+

Postobon. (2015). [Gráfico]. Consultado el 18 de mayo de 2020. Recuperado de https://www.postobon.com/

Real Academia Española. (2014). Diccionario de la lengua española. https://dle.rae.es/base#CiiosqO

Rebollo Delgado, L. (2008). Vida privada y protección de datos en la Unión Europea. Dykinson. http://www.digitaliapublishing.com.ezproxy.eafit.edu.co/visor/38093

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD). Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

(Reglamento general de protección de datos). 27 de abril de 2016. D.O. No. L 119 de 4.5.2016. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Reyes, L. (2019). La elaboración de perfiles en el contexto del marketing personalizado. Comunicaciones en propiedad industrial y derecho de la competencia, (86), 141-141. https://www.uria.com/documentos/publicaciones/6384/documento/Comunicaciones_86.pdf?id=8585

Rouse, M. (2015, enero). SearchDataCenter en español. TechTarget, SA de CV, 2018. https://searchdatacenter.techtarget.com/es/definicion/Base-de-datos

Sadin, E. (2019). La inteligencia artificial: el superyó del siglo XXI. Nueva Sociedad, (279), 141-148. https://nuso.org/media/articles/downloads/10.TC_Sadin_279.pdf

Schuh, J. (2020). Building a more private web: A path towards making third party cookies obsolete. https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html.

Smit, E., Van Noort, G. and Voorveld, H. (2014). Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe. Computers in Human Behavior, 32, 15–22. https://doi.org/10.1016/j.chb.2013.11.008

Superintendencia de Industria y Comercio de Colombia (2016). Concepto 16- 172268-00001-0000 del 9 de agosto de 2016.

Superintendencia de Industria y Comercio. (2018). Concepto Oficina Asesora Jurídica 18838-1.https://bit.ly/3mWaQH4

Superintendencia de Industria y Comercio (2020). Resolución 12192 del 1 de abril de 2020, "Por la cual se resuelve recurso de apelación". https://bit.ly/2S2UTRh

Unión Europea. (2020, agosto 24). Privacidad online. Consultado el 24 de agosto de 2020. https://bit.ly/3i2YQQk

Unión Europea. (2019, febrero 27). Derecho de la UE. Consultado el 2 de agosto de 2020. https://europa.eu/european-union/law_es

Universidad de Alicante. (2011, noviembre 2). *Cookies: ¿cómo funcionan?* [video]. YouTube. https://www.youtube.com/watch?v=hbObT3L3ND8&t=5s

Venegas Loaiza, A. (6 de julio de 2019). Colombia es el cuarto país en donde más horas al día se navega en internet. La República. https://www.larepublica.co/internet-economy/colombia-es-el-cuarto-pais-en-donde-mas-horas-al-dia-se-navega-en-internet-2881830