

ANUARIO DE  
**DERECHO  
PRIVADO**

MONOGRAFÍAS

**MAESTRÍA  
EN DERECHO  
PRIVADO**

**04**

**MARCELA CASTRO DE CIFUENTES**  
Directora

ANUARIO DE

# DERECHO PRIVADO

## 04

ISSN 2665-2714

Para citar: <http://dx.doi.org/10.15425/2017.309>

Fecha de publicación: agosto de 2022

### Ediciones Uniandes

Carrera 1.ª n.º 18A-12, bloque Tm

Bogotá D.C. Colombia

Teléfono: 3394949 ext. 2133

<http://ediciones.uniandes.edu.co>

[infeduni@uniandes.edu.co](mailto:infeduni@uniandes.edu.co)

Universidad de los Andes | Vigilada Mineducación.

Reconocimiento como Universidad: Decreto 1297 del 30

de mayo de 1964. Reconocimiento personería jurídica:

Resolución 28 del 23 de febrero de 1949, Minjusticia.

Acreditación institucional de alta calidad 10 años:

Resolución 582 del 9 de enero del 2015, Mineducación.



# Tratamiento de datos personales a través de *web cookies*: análisis bajo la legislación colombiana de protección de datos personales

ALEJANDRO LONDOÑO CONGOTE\*

DOI: <http://dx.doi.org/10.15425/2022.655>

**Resumen.** Las *web cookies* son un medio comúnmente utilizado para recolectar Datos personales en la internet. Se trata de dispositivos de almacenamiento y recuperación de Datos que se instalan en el equipo terminal de un usuario. En razón a que en sí mismas realizan una actividad de Tratamiento de Datos personales en el territorio colombiano, este artículo tiene como objetivo identificar las maneras como un Responsable que emplee esta tecnología podría vulnerar los deberes que emanan del principio de transparencia bajo la legislación de protección de Datos personales.

**Palabras claves:** *Web cookie*; Datos personales; Tratamiento; Autorización; transparencia; neutralidad tecnológica.

\* Abogado, Especialista en Derecho de la Empresa y Magister en Derecho Privado de la Universidad de los Andes. Asesor de la Delegatura para la Protección de Datos Personales en la Superintendencia de Industria y Comercio. Asistente Académico de la Especialización en Derecho Comercial de la Universidad de los Andes. Miembro del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Universidad de los Andes.

[a.londono13@uniandes.edu.co](mailto:a.londono13@uniandes.edu.co)

## Processing of personal data through *web cookies*: analysis under the colombian legislation on data protection

**Abstract.** *Web cookies* are a commonly use means of collecting Personal Data on the Internet. They are data storage and retrieval devices that are installed in a user's terminal device. Since they perform a processing of personal data in the Colombian territory, this article aims to identify the ways in which a Controller using this technology could violate the duties arising from the principle of transparency under the Colombian legislation on data protection.

**Keywords:** *Web cookie*; personal data; processing; consent; transparency; technology neutrality.

## Introducción

Cotidianamente las personas utilizan la internet para acceder a sus páginas favoritas, observar catálogos de sus preferencias, realizar compras y, entre otras, buscar información. Paralelamente, las organizaciones (privadas y públicas) utilizan mecanismos electrónicos para recolectar y tratar información para desarrollar sus funciones y actividades<sup>1</sup>. De aquello que recolectan, una porción importante son los Datos personales, definidos como “cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables”<sup>2</sup>.

Un medio empleado para la captura de Datos personales en la internet son las *web cookies*. Estas, en palabras simples, son dispositivos de almacenamiento y recuperación de Datos que se instalan en el equipo terminal de un usuario<sup>3</sup>. Es importante saber que existen diferentes tipos de *cookies* y estas, por su parte, son empleadas para diversas finalidades. A modo de ejemplo, se pueden utilizar con la finalidad de análisis o, también, para publicidad comportamental.

Como se mencionó, en la red están las *web cookies*, las cuales son empleadas por los Responsables del Tratamiento<sup>4</sup> para la recolección masiva de información. Monitorean las actividades de las personas. Por ejemplo, “con qué frecuencia y cuáles son los sitios web que visitan los Titulares; el número de «clics» introducidos por un visitante de una web; y, en general cualquier actividad que se realice en línea”<sup>5</sup>.

Las *cookies* permiten recolectar información en tiempo real sobre cómo actúan las personas en internet. Es decir, cuáles son las páginas que visitan; los contenidos que consumen; la hora, fecha y lugar de las actividades; la frecuencia de las visitas; qué compran en línea; entre otros<sup>6</sup>. Dejusticia<sup>7</sup> concluyó que la segunda fuente

- 1 Ana Garriga Domínguez, Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua Madrid: Dykinson, 2016, 25.
- 2 Ley 1581 de 2012, 18 de octubre de 2012. Diario Oficial No. 48.587.
- 3 “Guía sobre el uso de las cookies”, Agencia Española de Protección de Datos Personales, acceso el 8 de abril de 2021, <https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf>
- 4 El literal e) del artículo 3 de la Ley 1581 de 2012 define Responsable de Tratamiento como, “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”.
- 5 Garriga, Nuevos retos, 37.
- 6 Laura Daniela González Guerrero, “Control De Nuestros Datos Personales En La Era Del Big Data: El Caso Del Rastreo Web De Terceros”, Estudios Socio-Jurídicos 21, n° 1 (2019); 213, <https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941>.
- 7 Centro de estudios jurídicos y sociales localizado en Bogotá, Colombia, dedicado al fortalecimiento del Estado de Derecho y a la promoción de los derechos humanos en Colombia y en el Sur Global.

de información en Colombia son los Datos recolectados a través del *web tracking*<sup>8</sup>. Y, además, la herramienta más utilizada para esta finalidad son las *web cookies*<sup>9</sup>.

Por ejemplo, las tiendas venden e intercambian información sobre prácticas de consumo, como las ventas por catálogo; las suscripciones a revistas; ventas de automóviles; encuestas de mercadeo; tarjetas de clientes frecuentes; entre otras. Para poner esta situación en contexto, corredores de Datos como Oracle y Data-logix afirman “agregar y proveer información sobre más de 2 billones de dólares en consumo de 110 millones de hogares, proporcionada por 1500 socios de datos”<sup>10</sup>.

A través de las *cookies*, la información se transmite desde un servidor al navegador *web*<sup>11</sup> del usuario. Luego, se transmite al servidor cada vez que el usuario accede a la página de un servidor utilizando el mismo navegador<sup>12</sup>. De esta manera, el sitio *web* “sabe”, por ejemplo, en qué idioma el usuario desea ver su contenido o qué tipo de publicidad le gustaría ver<sup>13</sup>.

A título de ejemplo y con el fin de corroborar el extenso uso de esta tecnología en internet, la tabla a continuación muestra qué compañías —de las cuales son accionistas siete (7) de las personas más adineradas del mundo según la revista Forbes— utilizan *cookies* en sus plataformas digitales<sup>14</sup>.

---

Como centro de investigación-acción, nuestro objetivo es la promoción del cambio social realizando estudios rigurosos y propuestas sólidas de políticas públicas, adelantando campañas de incidencia en foros de alto impacto, litigios de interés público y diseñando e impartiendo programas educativos y de formación. Para más información acerca del centro se puede consultar en <https://www.dejusticia.org>

- 8 El *web tracking* es la práctica de recopilar puntos de información (datos) creados al navegar en sitios web, que pueden estar vinculados a una persona específica a través de un identificador de usuario. Vivian Newman Pont y Daniel Ospina Celis, Editors Data Feast. *Enterprises and Personal Data in Latin America* (Bogotá: Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia, 2020), 33.
- 9 Vivian Newman y María Paula Ángel, *Festín de datos Empresas y datos personales en América Latina* (Bogotá: Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia, 2020), 134.
- 10 González, *Control de nuestros datos*, 212.
- 11 La Real Academia de Ingeniería define navegador como, “*Aplicación informática que permite acceder y consultar fácilmente documentos en hipertexto, capaz de lanzar solicitudes de documentos HTML a los servidores web, y de recibir y presentar en pantalla estos documentos*”, acceso el 25 de abril de 2021, <http://diccionario.raing.es/es/lema/navegador-0>
- 12 Chuan Yue y Mengjun Xie, “An automatic HTTP cookie management system”. *Computer Networks, Estados Unidos de America* 54, n° 13 (2010): 2182, <https://doi.org/10.1016/j.comnet.2010.03.006>
- 13 Eleni Kost, “Peeking into the cookie jar: the European approach towards the regulation of cookies”. *International Journal of Law and Information Technology*, 21, n° 4 (2013): 380, <http://dx.doi.org/10.2139/ssrn.2675810>.
- 14 “Los 50 más ricos del mundo 2021”, Forbes Colombia, acceso el 12 de abril de 2021, <https://forbes.co/2021/04/09/editors-picks/los-50-mas-ricos-del-mundo-2021/>.

Persona	Compañía	Fuente	Uso de cookies
Jeff Bezos	Amazon.com, Inc.	Aviso de privacidad de Amazon <sup>15</sup>	Sí
Elon Musk	Tesla, Inc.	Aviso de Privacidad para los Clientes <sup>16</sup>	No
Bernard Arnault	Louis Vuitton Malletier SAS	Global Privacy Policy <sup>17</sup>	Sí
Bill Gates	Microsoft Corporation	Declaración de privacidad de Microsoft <sup>18</sup>	Sí
Mark Zuckerberg	Facebook Inc.	Cookies y otras tecnologías de almacenamiento <sup>19</sup>	Sí
Larry Ellison	Oracle Corporation	Oracle General Privacy Policy <sup>20</sup>	Sí
Larry Page	Alphabet (Google LLC)	Como utiliza Google las cookies <sup>21</sup>	Sí

Tabla 1. Algunas empresas que usan *web cookies*  
Elaborada por el autor.

Con todo lo anterior, la recolección masiva de información personal tiene un impacto directo en el conjunto de derechos que garantizan el debido Tratamiento de Datos personales<sup>22</sup>. Por ejemplo, es posible que un Responsable<sup>23</sup> no informe adecuadamente lo que hace con los Datos de las personas. A su vez, las políticas que se ponen a disposición del público pueden emplear un lenguaje ambiguo lo cual no ayuda a hacer transparentes los flujos de datos que suceden detrás de, a saber, la publicidad comportamental que se basa en Datos personales recolectados mediante *cookies*. Lo anterior lleva a concluir que no se puede considerar que el Titular<sup>24</sup> está “informado” si, por ejemplo, no tiene certeza sobre las implicaciones que trae el Tratamiento de su información.

15 “Aviso de privacidad de Amazon”, Amazon, acceso el 12 de abril de 2021, [https://www.amazon.com/-/es/gp/help/customer/display.html?nodeId=468496&ref\\_=footer\\_privacy#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40\\_\\_SECTION\\_0D132936501A4AE0A2F8D74426A8A2CA](https://www.amazon.com/-/es/gp/help/customer/display.html?nodeId=468496&ref_=footer_privacy#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40__SECTION_0D132936501A4AE0A2F8D74426A8A2CA).

16 “Privacy”, Tesla, acceso el 12 de abril de 2021, <https://www.tesla.com/about/legal?redirect=no>.

17 “Legal & Privacy”, Louis Vuitton, acceso el 12 de abril de 2021, <https://uk.louisvuitton.com/eng-gb/legal-privacy>

18 “Declaración de privacidad de Microsoft”, Microsoft, acceso el 12 de abril de 2021, <https://privacy.microsoft.com/es-mx/privacystatement>.

19 “Cookies y otras tecnologías de almacenamiento”, Facebook, acceso el 12 de abril de 2021, <https://www.facebook.com/policias/cookies/>.

20 “Privacy @ Oracle Oracle General Privacy Policy”, Oracle Legal, acceso el 12 de abril de 2021, <https://www.oracle.com/legal/privacy/privacy-policy.html>.

21 “Privacidad y Condiciones”, Google, acceso el 12 de abril de 2021, <https://policias.google.com/technologies/cookies?hl=es>.

22 Garriga, Nuevos retos, 35.

23 El literal e) del artículo 3 de la Ley 1581 de 2012 define Responsable del Tratamiento como “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”.

24 El literal f) del artículo 3 de la Ley 1581 de 2012 define Titular como “Persona natural cuyos datos personales sean objeto de Tratamiento”.

Colombia carece de regulación expresa sobre las *web cookies* y su uso para el rastreo de hábitos de navegación en línea mediante las denominadas *cookies*<sup>25</sup>. Pese a lo anterior, la Superintendencia de Industria y Comercio ha entendido que la regulación sobre Tratamiento de Datos personales debe aplicarse al margen de los procedimientos, metodologías o tecnologías que se utilicen para recolectar, usar o tratar ese tipo de información<sup>26</sup>. Y, por lo anterior, el Tratamiento de esa información por medio de *cookies* está sujeto a la regulación colombiana y su incumplimiento puede generar sanciones<sup>27</sup>. Bajo dicha premisa, surge la siguiente pregunta: ¿cómo podrían los Responsables del Tratamiento de Datos personales que usan *web cookies* para su recolección vulnerar los deberes que emanan del principio de transparencia?

Para responder la pregunta anterior, que plantea el objetivo de este texto, se emplea el método de investigación hermenéutico. Y, a su vez, se aplica la técnica sistemática, es decir, una interpretación que deduce el significado de una disposición puesta en el “sistema” del Derecho<sup>28</sup>. Finalmente, también se recurrirá a un método de análisis de Derecho comparado. Todo, con la intención de tener un marco de referencia sobre las obligaciones que derivan del principio de transparencia en documentos internacionales.

- 25 “Documento CONPES 4012 Política Nacional de Comercio Electrónico”, Departamento Nacional de Planeación, acceso el 19 de abril de 2021, <https://colaboracion.dnp.gov.co/CDT/Conpes/Economicos/4012.pdf>
- A diferencia de Colombia, en Europa sí está regulada esta tecnología. Precisamente, se encuentra la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 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).
- 26 Superintendencia de Industria y Comercio, Resolución N° 62132 del 5 de octubre de 2020 (Por medio de la cual se emiten ordenes administrativas a las sociedades ByteDance Ltd., TikTok, Inc. y TikTok Pte. Ltd.).
- 27 El artículo 23 de la Ley 1581 de 2012 establece que, “*La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones: a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó; b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar; c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio; d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles; PARÁGRAFO. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva*”.
- 28 Óscar Alexis Agudelo-Giraldo, *La pregunta por el método: derecho y metodología de la investigación* (Bogotá: Editorial Universidad Católica de Colombia, 2018), 29.

# I. Web cookies, neutralidad tecnológica y tratamiento de datos personales

Dentro del presente capítulo se describirán qué son las *web cookies*. Posteriormente se realizará una clasificación de éstas y, por último, se expondrá las implicaciones jurídicas del uso de *cookies* para tratar Datos personales.

## 1. Las web cookies

La creación de las *web cookies* (en adelante *cookies*) está relacionada con la mercantilización de la internet. En 1994 Netscape, una sociedad comercial, implementó las *cookies* en su página *web*. Lou Montulli, el ingeniero de software que trabajó para esa compañía pretendía darle memoria a la *web*<sup>29</sup>. Lo anterior, toda vez que el protocolo HTTP<sup>30</sup> (conexión entre el cliente y el servidor) termina una vez se cierra la conexión. Es decir, finalizada la conexión entre el servidor y el cliente no queda registro. Entonces, las *cookies* fueron desarrolladas principalmente para proveer continuidad del servidor *web*<sup>31</sup> con las transacciones del usuario<sup>32</sup>.

Las *cookies*<sup>33</sup> son pequeños archivos de texto que un servidor le puede remitir a un buscador<sup>34</sup>. El buscador guarda el archivo. En caso de que el buscador realice nuevamente un contacto con ese mismo servidor, procederá a remitir de

29 “Darle memoria a la *web*” es una frase empleada en Paul Schwartz, “Internet Privacy and the State”. Connecticut Law Review n° 32 (2000) 815, <http://dx.doi.org/10.2139/ssrn.229011>.

30 El protocolo de transferencia de hipertexto es el protocolo desarrollado para la internet. El protocolo permite las comunicaciones entre los servidores *web* y las páginas *web*.

31 De acuerdo con la Real Academia de Ingeniería, un servidor *web* es “un software servidor que utiliza el protocolo *http* para suministrar documentos en formato *HTML*, junto con sus *scripts* y archivos asociados, cuando lo solicite algún cliente, como por ejemplo, algún explorador *web*”, acceso el 20 de abril de 2021, <http://diccionario.raing.es/es/lema/servidor-http-0>.

32 Laura McCarthy y Dave Yates, “The use of cookies in Federal agency web sites: Privacy and recordkeeping issues”. Government Information Quarterly 27, n° 3 (2010): 232, <https://doi.org/10.1016/j.giq.2010.02.005>.

33 Lou Montulli, el ingeniero de software que trabajó para Netscape y afirmó haber desarrollado originalmente las *cookies*, describe la *cookie* como un fragmento de datos que se almacena, luego el servidor lo entrega al cliente, el cliente lo almacena y lo devuelve al servidor cada vez que el cliente regresa. Ídem.

34 El proceso de las *cookies* conlleva dos pasos. El primer paso es recibir la *cookie*, lo que se facilita mediante un programa del servidor que contiene una respuesta de encabezado “Set- Cookie” a una solicitud HTTP. El segundo paso del proceso es el “retiro” de la *cookie* que ocurre cuando un navegador accede a una URL y coincide con la del encabezado Set-Cookie. En ese momento, cualquier información que se encuentre en las *cookies* se envía al servidor *web*. Ídem.

regreso el archivo de información. Así, el servidor puede reconocer el buscador<sup>35</sup>. Por ejemplo, se presta, entre otras, para recordar contenido de un carro de compras en línea.

Ahora bien, almacenar la información que recolectan las *cookies* en los servidores *web* implicaría la saturación de estos. Por eso, se acude al almacenamiento de algunos de estos archivos de texto en el disco duro<sup>36</sup> del usuario. Es decir, las *cookies* también se incorporan o instalan en los dispositivos de las personas.

En este orden de ideas, una *cookie* es “*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 información ya almacenada*”<sup>37</sup>. Como explica la doctrina, la internet sin *cookies* sería como tener que ir a la caja cada vez que uno coloca un artículo en su carrito de compras<sup>38</sup>.

Algunas categorías de información que pueden llegar a almacenar estos dispositivos son las siguientes: Identificación y perfil del usuario; dirección IP<sup>39</sup>; contenido del carrito de compras; preferencias seleccionadas por el usuario; números de serie del dispositivo del usuario; frecuencia de contacto con empresas e historial de compras<sup>40</sup>; etc. A manera de ejemplo, la Política de Privacidad de Facebook Inc. indica que se recolecta la siguiente información por medio de las *cookies*.

Facebook utiliza *cookies* “*si tienes una cuenta de Facebook, utilizas los Productos de Facebook, como nuestro sitio web y nuestras apps, o visitas otros sitios web y apps que usan los Productos de Facebook*”<sup>41</sup>. En aquellas situaciones, se recolecta, entre otras, la siguiente información de los Titulares: la ubicación de una foto o la fecha de creación de un archivo; Datos sobre cómo usa el usuario el sitio *web*; el tiempo de permanencia en su página *web*; la ubicación del Titular; si el usuario ha

35 Frederik Zuiderveen, *Improving Privacy Protection in the Area of Behavioural Targeting* (Amsterdam: Wolters Kluwer, 2015), 23.

36 De acuerdo con la Real Academia de Ingeniería un “disco duro” es un “*disco magnético con soporte rígido y cuyas cabezas vuelan muy cerca del mismo sin tocarle*”, acceso el 21 de abril de 2021, <http://diccionario.raing.es/es/lema/disco-duro>.

37 “Guía sobre el uso de las *cookies*”, Agencia Española de Protección de Datos, acceso el 12 de abril de 2021 <https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf>

38 Hal Berghel, “Digital Village: Caustic *cookies*”. *Communications of the ACM* 44, n° 5 (2001): 19, <https://doi.org/10.1145/374308.374320>.

39 De acuerdo con la Real Academia Española una “dirección IP” es la “*identificación numérica de un elemento conectado a una red que utiliza el protocolo TCP/IP*”, acceso el 10 de diciembre de 2020, <https://dpej.rae.es/lema/dirección-ip>.

40 McCarthy, *The use of cookies in Federal agency web sites*, 233.

41 “*Cookies y otras tecnologías de almacenamiento*”, Facebook, acceso el 12 de abril de 2021, <https://www.facebook.com/policies/cookies/>

visitado el sitio *web* de un negocio, compraron sus productos o usaron sus aplicaciones<sup>42</sup>; la frecuencia con la que se compra un producto después de ver la impresión de un anuncio; entre otras.

### 1.1. Clasificación de las *web cookies*

Se pueden clasificar, entre otras, por: i) el tipo de entidad que las gestiona; ii) su finalidad; iii) el tiempo que permanecen activas; y, iv) su capacidad de engaño.

Clasificación de las <i>cookies</i>			
Según la entidad que las gestiona	Según su finalidad	Según el tiempo que permanecen activas	Según su capacidad de engaño
1. Propias 2. De terceros	1. Técnicas 2. Preferencias/personalización 3. Análisis 4. Publicidad comportamental	1. De sesión 2. Persistentes	1. <i>Zombie Cookies</i> 2. <i>Flash Cookies</i>

Tabla 2. Clasificación de las *cookies*  
Elaborada por el autor.

#### 1.1.1. Según la entidad que las gestiona

Esta clasificación tiene como objetivo identificar el sujeto que gestiona el dominio desde donde se envían las *cookies* y se tratan los Datos que son recolectados. En este sentido, se pueden distinguir entre las *cookies* propias y las de terceros. Las primeras, hacen referencia a las que son enviadas al equipo terminal del Titular<sup>43</sup> desde un dominio operado por el propio dueño de la página *web*<sup>44</sup> y desde el que se presta el servicio solicitado por el Titular de la información<sup>45</sup>.

42 De acuerdo con la Real Academia de Ingeniería una aplicación es un “*software programado que ejecuta una determinada función en el sistema de información*”, acceso el 21 de abril de 2021, <http://diccionario.raing.es/es/lema/aplicación>.

43 En el literal f) del artículo 3 de la Ley 1581 de 2012 se define titular como la “*Persona natural cuyos datos personales sean objeto de Tratamiento*”.

44 Las *cookies* han estado asociadas a las páginas *web*. Sin embargo, esta tecnología es actualmente empleada tanto en páginas *web* como en otro tipo de plataformas y aplicaciones (por ejemplo, las aplicaciones para teléfonos inteligentes). A lo largo de este texto se utilizará el término página *web* para englobar todos estos posibles medios.

45 “Guía sobre el uso de las *cookies*”, Agencia Española de Protección de Datos, acceso el 10 de abril de 2021, <https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf>

Por su parte, las *cookies* de terceros son las que se envían al equipo terminal del Titular desde un dominio que no es operado por el dueño de la página *web*, sino por otro Responsable<sup>46</sup> que trata los Datos obtenidos a través de las *cookies*<sup>47</sup>.

En razón a la clasificación desarrollada, es importante tener presente lo siguiente:

Primero, es posible que las *cookies* sean remitidas desde un dominio operado por el propio dueño de la página *web*, pero la información recolectada sea tratada por un tercero. En este caso, se está frente a *cookies* de terceros toda vez que quien define las finalidades del Tratamiento no es el dueño de la página, sino el tercero.

Segundo, la clasificación de estas *cookies* se hace importante toda vez que, en el caso de un indebido Tratamiento de Datos personales identificado por el Titular o la autoridad de protección de Datos, será de vital importancia poder identificar quién es el Responsable o los corresponsables del Tratamiento.

### 1.1.2. Según su finalidad

Como se mencionó previamente, existen diversos propósitos para el uso de las *cookies*. En primer lugar, las *cookies* técnicas hacen referencia a aquellas que le permiten al Titular la navegación a través de una página *web*, aplicación o plataforma. De igual forma, le permiten al Titular la utilización de diferentes opciones o servicios que en ella existen. Por ejemplo, en las páginas dedicadas al comercio electrónico, la función del “carrito de compras”, como se mencionó, es posible gracias a estas *cookies*<sup>48</sup>.

De ahí que, las *cookies* técnicas están relacionadas con la gestión y operatividad de la página *web*, a saber:

“control del tráfico, la comunicación de datos, identificación de la sesión, acceso a partes de acceso restringido, recordación de los elementos que integran el pedido del usuario, el proceso de compra, gestión de pago, control del fraude vinculado a la seguridad, contar las visitas a efectos de facturación de licencias de software”<sup>49</sup>.

Las *cookies* de preferencias, por su parte, permiten recordar información para que el Titular acceda al servicio con determinadas características que pueden

46 En el literal e) del artículo 3 de la Ley 1581 de 2012 se define Responsable como la “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”.

47 Ídem.

48 “Guía sobre el uso de las *cookies*”, Agencia Española de Protección de Datos, acceso el 10 de abril de 2021, <https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf>

49 Ídem.

diferenciar su experiencia de la de otros Titulares. Como, por ejemplo, entre otras posibilidades está: *“el idioma, el número de resultados a mostrar cuando el usuario realiza una búsqueda, el aspecto o contenido del servicio en función del tipo de navegador a través del cual el usuario accede al servicio o de la región desde la que accede al servicio, etc.”*<sup>50</sup>.

De otra parte, las *cookies* de análisis *“son aquellas que permiten al responsable de las mismas el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas, incluida la cuantificación de los impactos de los anuncios”*<sup>51</sup>. Este tipo de *cookies* pueden ser tratadas por el dueño de la página web o también por un tercero. En últimas, le permiten al Responsable estudiar la navegación que hacen los Titulares dentro de sus páginas web. Por regla general, estas *cookies* no están asociadas a ningún Dato de carácter personal porque la información recopilada se proyecta de forma anónima.

En línea con lo anterior, el Grupo de Trabajo del Artículo 29<sup>52</sup> considera que es poco probable que estas *cookies* representen un riesgo para la privacidad de los Titulares<sup>53</sup>. Lo anterior, siempre que se trate de *cookies* de análisis propias. No obstante, es importante que los Responsables les faciliten a los Titulares suficiente información sobre su uso, y se incluya la posibilidad de que estos últimos manifiesten su negativa o inconformidad sobre su utilización.

Por último, las *cookies* de publicidad comportamental<sup>54</sup> son aquellas *“que almacenan información del comportamiento de los usuarios obtenida a través de la*

50 Ídem.

51 Ídem.

Es importante anotar que la información recogida mediante este tipo de *cookies* se utiliza en la medición de la actividad de los sitios web, aplicación o plataforma, con el fin de introducir mejoras en función del análisis de los datos de uso que hacen los usuarios del servicio.

52 El Grupo de Trabajo del artículo 29 (GT Art. 29) fue el grupo de trabajo europeo independiente que se ocupó de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018, cuando entró en vigor Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016. El grupo estaba compuesto por un representante de la autoridad de protección de datos de cada Estado miembro de la UE, el Supervisor Europeo de Protección de Datos y la Comisión Europea. Se pueden consultar todas las noticias archivadas sobre el grupo en <https://ec.europa.eu/newsroom/article29/news-overview.cfm>.

53 “Cookie sweep combined analysis report”, Grupo de Trabajo del Artículo 29, acceso el 10 de abril de 2021, [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwicwNOpksztAhXmQd8KHfQPBClQFjABegQIARAC&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fdocument.cfm%3Faction%3Ddisplay%26doc\\_id%3D56123&usq=AOvVaw1GeyzU33CSutUzfCODzNbf](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwicwNOpksztAhXmQd8KHfQPBClQFjABegQIARAC&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fdocument.cfm%3Faction%3Ddisplay%26doc_id%3D56123&usq=AOvVaw1GeyzU33CSutUzfCODzNbf)

54 De acuerdo con la Unión Internacional de Telecomunicaciones para el 2020, más del 90 por ciento de la población tenía acceso a una red de banda ancha móvil (3G o superior). Por su parte, para el año 2019 habían 1.72 billones de páginas web en la internet. De estas, la gran mayoría requieren acudir a medios de financiación para poder ofrecer contenido sin requerir una contraprestación

*observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo*<sup>55</sup>.

### 1.1.3. Según el tiempo que permanecen activas

Por otro lado, se encuentra la clasificación de las *cookies* según el tiempo que permanecen activas en el equipo terminal del Titular. En esta clasificación se pueden diferenciar entre las *cookies* de sesión y las persistentes. Las primeras hacen referencia a aquellas “(...) diseñadas para recolectar y almacenar datos mientras el usuario accede a una página web”.

Habitualmente, las *cookies* de sesión se utilizan para almacenar información que solo interesa conservar para la prestación del servicio solicitado por el usuario en una sola ocasión (lista de productos adquiridos) y son eliminadas al terminar la sesión.

Por su parte, las *cookies* persistentes “son aquellas en las que los datos siguen almacenados en el terminal [equipo del titular] y pueden ser accedidos y tratados durante un periodo definido por el responsable de la cookie, y que puede ir de unos minutos a varios años”<sup>56</sup>.

Previo al diseño y desarrollo del producto en el que se utilizará este tipo de *cookies* es importante valorar si es estrictamente necesaria su implementación. Esto, debido a que los riesgos asociados al debido Tratamiento de la información podrían reducirse mediante la utilización de *cookies* de sesión. Ahora bien, en caso de considerarse necesario y apropiado el uso de *cookies* persistentes, se recomienda reducir al mínimo su duración atendiendo a la finalidad de uso informada a los Titulares<sup>57</sup>.

Esta variedad de *cookies* es frecuentemente utilizada por las empresas. Así, por ejemplo, verificando la información de las empresas de la Tabla 1, constatamos que aquellas utilizan la gran mayoría de las clases de *cookies* señalada en la Tabla 2.

---

económica por parte de los usuarios. Es así como para poder ofrecer contenido sin contraprestación económica de los usuarios, muchas páginas *web* son financiadas por la utilidad que genera la publicidad comportamental. “Measuring digital development. Facts and figures. 2020”, Unión Internacional de Telecomunicaciones, acceso el 5 de abril de 2021, <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2020.pdf>

55 “Guía sobre el uso de las cookies”, Agencia Española de Protección de Datos, acceso el 10 de abril de 2021, <https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf>

56 Ídem.

57 Ídem.

#### 1.1.4. Según su capacidad de engaño

Finalmente, se encuentra la clasificación de las *cookies* según su capacidad de engaño. Algunos Responsables acuden a mecanismos que sin el conocimiento de los Titulares recolectan sus Datos personales<sup>58</sup>. Un ejemplo de estos mecanismos engañosos son las denominadas *zombie Cookies* y las *flash cookies*.

Las primeras, son aquellas que si bien aparentan estar eliminadas no lo están. Precisamente, se encuentran ocultas en el dispositivo terminal para que, una vez el Titular acceda nuevamente al sitio que las instaló originalmente, puedan activarse y recolectar una vez más la información. También puede suceder que el Titular identifique la *cookie* y proceda con la supresión. No obstante, por lo que ya no puede rastrearse, la *cookie* simplemente se recrea y continúa rastreando<sup>59</sup>.

Por su parte, las *flash cookies* son archivos que se almacenan en la memoria interna de la aplicación Adobe Flash Player en lugar de la carpeta estándar de *cookies*. Como resultado, estas son más difíciles de localizar y eliminar. En adición, no siempre serán eliminadas cuando el Titular borra manualmente sus *cookies*. Asimismo, es de anotar que las diversas extensiones en los navegadores para bloquear las *cookies* no han resultado completamente efectivas para evitar la instalación de estas<sup>60</sup>.

## 2. Neutralidad tecnológica

La regulación sobre Tratamiento de Datos personales debe aplicarse al margen de los procedimientos, metodologías o tecnologías que se utilicen para recolectar, usar o tratar ese tipo de información<sup>61</sup>. Es decir, la ley colombiana permite el uso de tecnologías para tratar Datos personales. Sin embargo, al mismo tiempo, exige que se haga de manera respetuosa del ordenamiento jurídico.

58 Joseph Newman, “Cookie Monsters: Locally Stored Objects, User Privacy, and Section 1201 of the DMCA,” *AIPLA Quarterly Journal* 41, no. 3 (2013): 519.

59 Ídem.

60 Alexandra Drury, “How Internet User’s Identities Are Being Tracked and Used,” *Tulane Journal of Technology and Intellectual Property* 15 (2012): 223, [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjrvJSO3P32AhWASTABHUCjBoMQFnoECAkQAQ&url=https%3A%2F%2Fjournals.tulane.edu%2FTIP%2Farticle%2Fview%2F2613%2F2435&usq=AOvVaw0Cavq5Ow\\_semk61MjRVYAm](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjrvJSO3P32AhWASTABHUCjBoMQFnoECAkQAQ&url=https%3A%2F%2Fjournals.tulane.edu%2FTIP%2Farticle%2Fview%2F2613%2F2435&usq=AOvVaw0Cavq5Ow_semk61MjRVYAm)

61 Superintendencia de Industria y Comercio, Resolución N° 62132 del 5 de octubre de 2020 (Por medio de la cual se emiten ordenes administrativas a las sociedades ByteDance Ltd., TikTok, Inc. y TikTok Pte. Ltd.).

Esto ha sido reiterado por la Superintendencia de Industria y Comercio. Al respecto, en la Resolución N° 38281 de 14 de julio de 2020<sup>62</sup> afirmó:

“La Ley Estatutaria 1581 de 2012 es neutral tecnológica y temáticamente. Ello significa que aplica a cualquier Tratamiento con independencia de las técnicas, procesos o tecnologías —actuales o futuras— que se utilicen para dicho efecto. Por ende, debe observarse en la recolección, uso y Tratamiento de datos personales para diversos fines (marketing, políticos, cobro de cartera, etc.) mediante el uso de técnicas o herramientas como “marcadores predictivos”, “robocalls”, “nuisance calls” e inteligencia artificial (IA)”.

Más aún, la importancia de la neutralidad tecnológica fue reiterada recientemente por la Organización de Estados Americanos (en adelante OEA). En efecto, el pasado 9 de abril de 2021, el Comité Jurídico Interamericano (CJI), órgano consultivo de la OEA, aprobó por unanimidad los “Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones”. Allí, se pone de presente que los principios son de aplicación neutral frente al Tratamiento de datos con cualquier tecnología presente o futura procurando “*que las normas sigan siendo ‘tecnológicamente neutrales’ y no se vuelvan obsoletas como consecuencia de los rápidos cambios tecnológicos*”<sup>63</sup>.

De esta manera, los Responsables del Tratamiento que usen “innovaciones tecnológicas”, como lo son las *cookies*, deben cumplir todas las normas sobre Tratamiento de Datos personales.

### 3. Implicaciones jurídicas del uso de *cookies* para tratar datos personales

Como se mencionó, mediante el uso de *cookies* se recolectan, según el caso, Datos personales como, entre otros, los siguientes: nombre de usuario; fecha de nacimiento; dirección de correo electrónico y/o número de teléfono; información que el Titular divulgue en su perfil de usuario; así como la fotografía o video de perfil.

62 Por medio de la cual se resuelve el recurso de apelación de la sociedad Mervicol S.A.S

63 Comité Jurídico Interamericano. Documento CJI/RES. 266 (XCVIII/21) del 9 de abril de 2021.

La Red Iberoamericana de Protección de Datos<sup>64</sup> ha reconocido que,

“(…) aunque cada día el mundo es más transfronterizo, global e hiperconectado, ello no significa que las normas nacionales sobre Tratamiento de datos personales hayan desaparecido o que no sean de obligatorio cumplimiento. Por eso, para que su producto (…) no sea objetado o cuestionado jurídicamente es muy relevante que desde el inicio realice un estudio de riesgos legales de las regulaciones nacionales”<sup>65</sup>.

En sintonía con lo anterior, la Corte Constitucional ha destacado que las actividades en la Internet no se sustraen del respeto de los mandatos constitucionales. Por eso concluyó que,

“en Internet (…) puede haber una realidad virtual, pero ello no significa que los derechos, en dicho contexto, también lo sean. Por el contrario, no son virtuales: se trata de garantías expresas por cuyo goce efectivo en el llamado “ciberespacio” también debe velar el juez constitucional”<sup>66</sup>.

Así mismo, la Corte Constitucional afirma que, “*nadie podría sostener que, por tratarse de Internet, los usuarios sí pueden sufrir mengua en sus derechos constitucionales*”<sup>67</sup>.

Bajo las premisas desarrolladas, la Superintendencia de Industria y Comercio (Autoridad de Protección de Datos Personales en Colombiana) ha reiterado que las *cookies* son un medio de recolección de Datos personales<sup>68</sup>. De ahí que, los Responsables que empleen las *cookies* para recolectar información personal deben cumplir la legislación colombiana.

64 La Red Iberoamericana de Protección de Datos (RIPD) fue creada el 6 de junio de 2003 con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en La Antigua, Guatemala. Actualmente está integrada por 16 autoridades de protección de datos y 18 observadores dentro de los cuales se destacan la Organización de Estados Americanos (OEA), El Supervisor Europeo de Protección de Datos, el Comité Consultivo del Convenio 108, entre otros. Página web: <https://www.redipd.org/es>

65 “Recomendaciones Generales para el Tratamiento de Datos Personales en la Inteligencia Artificial”, Red Iberoamericana de Protección de Datos Personales, acceso el 1 de abril de 2021, [https://www.sic.gov.co/sites/default/files/files/pdf/1%20RIPD%20\(2019\)%20RECOMENDACIONES%20GENERALES%20PARA%20EL%20TRATAMIENTO%20DE%20DATOS%20EN%20LA%20IA.pdf](https://www.sic.gov.co/sites/default/files/files/pdf/1%20RIPD%20(2019)%20RECOMENDACIONES%20GENERALES%20PARA%20EL%20TRATAMIENTO%20DE%20DATOS%20EN%20LA%20IA.pdf)

66 Corte Constitucional, sentencia C-1147 del 31 de octubre de 2001. M.P. Manuel José Cepeda Espinosa.

67 Ídem.

68 Ver: Superintendencia de Industria y Comercio, Resolución N° 12192 del 1 de abril de 2020 (Por medio de la cual se resuelve el recurso de apelación de la sociedad Facebook Inc.), Resolución N° 53593 del 3 de septiembre de 2020 (Por medio de la cual se emiten ordenes administrativas a la sociedad Google LLC) y la Resolución N° 62132 del 5 de octubre de 2020 (Por medio de la cual se emiten ordenes administrativas a las sociedades ByteDance Ltd., TikTok, Inc. y TikTok Pte. Ltd.).

La Constitución Política de Colombia en su artículo 15 establece que todas las personas tienen derecho “(...) a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas”. Pero, también es enfática cuando afirma que, “En la recolección, Tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución”. Es decir, en cualquier operación sobre Datos personales debe respetarse la libertad y demás garantías consagradas en la legislación.

Ahora bien, la Ley Estatutaria 1581 de 2012 desarrolla el derecho constitucional al debido Tratamiento de Datos personales. En su artículo 2 dispone que:

“La presente ley aplicará al Tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales”.

A punto seguido, el artículo 3 afirma que:

“Para los efectos de la presente ley, se entiende por:

(...)

g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión”.

Así las cosas, la Ley Estatutaria 1581 de 2012 es aplicable cuando:

“El Tratamiento lo realiza el responsable o encargado, domiciliados o no en territorio colombiano, que directa o indirectamente, a través de cualquier medio o procedimiento, físico o electrónico, recolecta, usa, almacena o trata Datos personales en el territorio de la República de Colombia. Las anteriores hipótesis son ejemplos de “Tratamiento [sic] de datos [sic] personales efectuado en territorio colombiano” a que se refiere la parte primera del mencionado artículo 2.

El Responsable o el Encargado no está domiciliado en la República de Colombia ni realiza Tratamiento de Datos dentro del territorio colombiano. Pero, existen normas o tratados internacionales que los obliga a cumplir la regulación colombiana”<sup>69</sup>.

Entonces se reitera que, una *cookie* es un mecanismo que se instala en los equipos o dispositivos (bien sea celular; computador portátil; u otro) de los Titulares que residen o se domicilian en un territorio, en este caso la República de Colombia, con

69 Superintendencia de Industria y Comercio, Resolución N° 12192 del 1 de abril de 2020 (Por medio de la cual se resuelve el recurso de apelación de la sociedad Facebook Inc.).

el objetivo de recolectar algunos de sus Datos personales. En consecuencia, al realizarse un Tratamiento de información personal en el territorio colombiano, aquel se sujeta a las disposiciones de la Ley 1581 de 2012.

## II. Principio de transparencia en el tratamiento de datos personales

Dentro del presente capítulo se desarrollará, en primer lugar, el principio de transparencia en documentos internacionales. Y, posteriormente, se expondrá el principio de transparencia en la legislación nacional. Lo anterior, con el propósito de entender cuáles son los deberes que derivan de dicho principio.

### 1. El principio de transparencia en documentos internacionales

Son varios los documentos internacionales que desarrollan los postulados del principio de transparencia. Este contempla lo relacionado con el acceso a la información del Titular y, también brinda claridad sobre aspectos medulares relacionados con el Tratamiento de los Datos y los derechos que sobre él recaen.

Documento	Principio de transparencia
<b>Convenio 108 de 1981</b>	<p>Artículo 8° - Garantías complementarias para la persona concernida.</p> <p>Cualquier persona deberá poder:</p> <p>Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad Responsable del fichero.</p>
<b>Marco de Privacidad APEC (2004)</b>	<p>Aviso</p> <p>15. Controladores de Información Personal deben proporcionar declaraciones claras y de fácil acceso acerca de sus prácticas y políticas por lo que respecta a la información personal, que deben incluir: a) el hecho de que información personal está siendo recopilada; b) los propósitos para los que se está recopilando la información personal; c) los tipos de personas u organizaciones a las que se les podría revelar la información personal; d) la identidad y ubicación del controlador/ director de información personal, incluyendo información de cómo contactarlos respecto a sus prácticas y manejo de la información personal; e) la elección de medios que el controlador/ director de la información personal ofrece a los individuos para limitar el uso, revelación, acceso y corrección de su información.</p> <p>16. Todos los pasos razonablemente viables deberán ser tomados para asegurar que se proporcione el aviso antes o al momento de recopilar la información personal. De lo contrario, dicho aviso deberá ser proporcionado tan pronto como sea factible.</p>

*Continúa*

<p><b>Resolución de Madrid (2009)</b></p>	<p>Principio de Transparencia.</p> <p>1. Toda persona responsable deberá contar con políticas transparentes en lo que a los Tratamientos de datos de carácter personal que realice se refiere.</p> <p>2. La persona responsable deberá facilitar a los interesados, al menos, información acerca de su identidad, de la finalidad para la que pretende realizar el Tratamiento, de los destinatarios a los que prevé ceder los datos de carácter personal y del modo en que los interesados podrán ejercer los derechos previstos en el presente Documento, así como cualquier otra información necesaria para garantizar el Tratamiento leal de dichos datos de carácter personal.</p> <p>5. Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos Tratamientos dirigidos específicamente a menores de edad.</p> <p>6. Cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones establecidas en el presente apartado podrán satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos.</p>
<p><b>Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales (2013)</b></p>	<p>Principio de transparencia. Debería haber una política general de transparencia en lo concerniente al Tratamiento, el uso y las políticas relativas a los datos personales. Se deberían poner los medios para establecer la existencia y la naturaleza de los datos personales, así como los fines principales para los que se van a usar, así como la identidad y el domicilio habitual del inspector de datos.</p>
<p><b>Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016</b></p>	<p>Artículo 5. Principios relativos al Tratamiento.</p> <p>1. Los datos personales serán:</p> <p>a. Tratados de manera lícita, leal y transparente en relación con el interesado (licitud, lealtad y transparencia).</p> <p>Artículo 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.</p> <p>El responsable del Tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al Tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.</p>
<p><b>Convenio 108+ de 2018</b></p>	<p>Artículo 8. Transparencia en el Tratamiento.</p> <p>1. Cada Parte dispondrá que el Responsable del Tratamiento informe a los interesados de:</p> <p>a. Su identidad y residencia habitual o establecimiento;</p> <p>b. La base legal y los propósitos del Tratamiento previsto;</p> <p>c. Las categorías de datos personales tratados;</p> <p>d. Los destinatarios o categorías de destinatarios del datos personales, si los hubiera; y</p> <p>e. Los medios para ejercer los derechos establecidos en el artículo 9, así como cualquier información adicional necesaria para garantizar un Tratamiento justo y transparente de los datos personales.</p> <p>2. El apartado 1 no se aplicará cuando el Titular ya disponga de la información pertinente.</p> <p>3. Cuando los datos personales no se recopilen de los Titulares, el Responsable del Tratamiento no estará obligado a proporcionar dicha información cuando el Tratamiento esté expresamente prescrito por la ley o resulte imposible o implique esfuerzos desproporcionados.</p>

Continúa

<p><b>Principios actualizados sobre la privacidad y la protección de datos personales, con anotaciones (2021)</b></p>	<p>Principio dos. Transparencia y Consentimiento</p> <p>Antes o en el momento en que se recopilen, se deberían especificar la identidad y datos de contacto del responsable de los datos, las finalidades específicas para las cuales se tratarán los datos personales, el fundamento jurídico que legitima su Tratamiento, los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información a ser transmitida y los derechos del titular en relación con los datos personales a ser recopilados. Cuando el Tratamiento se base en el consentimiento, los datos personales solamente deberían ser recopilados con el consentimiento previo, inequívoco, libre e informado de la persona a que se refieran.</p>
---	--

Tabla 3. El principio de transparencia en documentos internacionales sobre Tratamiento de datos personales

Elaborada por el autor.

Es pertinente destacar lo siguiente de la tabla anterior:

Primero, el principio de transparencia exige que toda información relativa al Tratamiento de los Datos personales sea fácilmente accesible y de simple entendimiento. Para esto, es necesario que el Responsable utilice un lenguaje sencillo y claro. Si esto se logra, los Titulares podrán conocer los riesgos, las normas y los derechos que rodean el Tratamiento de su información.

Lo anterior cobra mayor relevancia cuando se considera la complejidad tecnológica y la capacidad del Titular para saber y comprender si se están recogiendo, por quién<sup>70</sup> y con qué fin, sus Datos personales.

Por último, es deber del Responsable actuar de forma transparente al tratar los Datos para garantizar un Tratamiento justo y permitir que los Titulares comprendan y, por lo tanto, ejerzan plenamente sus derechos en el contexto de dicho Tratamiento de datos. Es así como cierta información esencial debe ser proporcionada obligatoriamente de manera proactiva por el Responsable a los Titulares cuando directa o indirectamente recopile sus Datos.

## 2. El principio de transparencia en la legislación nacional

De acuerdo con el literal e) del artículo 4º de la Ley 1581 de 2012, el principio de transparencia implica que, *“en el Tratamiento debe garantizarse el derecho del*

70 Al respecto, la Superintendencia de Industria y Comercio mediante Resolución N° 53593 del 3 de septiembre de 2020 precisó que, *“Para garantizar que el menor de edad sea debidamente informado de lo que ordena la Ley es imprescindible que el Responsable del Tratamiento le proporcione esa información de manera sencilla y que los términos de la redacción sean comprensibles para niños, niñas y adolescentes. No es sensato, que el menor de edad se vea obligado a revisar varios links o enlaces. No es transparente que se diseñe un mecanismo para obligar a que el menor de edad tenga que realizar un “paseo” en varios sitios de la página web.”*

*Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan*". La redacción del citado artículo quedó limitada al acceso a que hace referencia el artículo 15 de la Constitución Política de Colombia, cuando afirma que las personas tienen derecho a *conocer* los datos que sobre ellas están en bases de datos o archivo.

Dado lo anterior, la Corte Constitucional en Sentencia C-748 de 2011 amplió su alcance en los siguientes términos:

"(...) debe precisarse que la información que debe ofrecerse al Titular de los datos debe ser cualificada y por tanto cuando procese datos personales, el Responsable o Encargado del Tratamiento de datos debe ofrecer, como mínimo, la siguiente información a la persona afectada: (i) información sobre la identidad del controlador de datos, (ii) el propósito del procesamiento de los datos personales, (iii) a quien se podrán revelar los datos, (iv) cómo la persona afectada puede ejercer cualquier derecho que le otorgue la legislación sobre protección de datos, y (v) toda otra información necesaria para el justo procesamiento de los datos".

Así las cosas, el principio de transparencia no puede entenderse solamente como una obligación que comprende contarle al Titular qué Datos se tienen sobre él. Ya que, también exige actos positivos y proactivos por parte del Responsable para garantizarle al Titular claridad sobre aspectos relevantes en cuanto al Tratamiento y sus derechos.

En Colombia, los deberes de información<sup>71</sup> que derivan del principio de transparencia se materializan, entre otras, de la siguiente manera:

## 2.1. Del derecho de acceso

Como se mencionó, la redacción del principio hace referencia al derecho de acceso establecido en el artículo 15 de la Constitución Política de Colombia. Es decir, la obligación que comprende contarle al Titular qué Datos se tiene almacenados sobre él.

Por su parte, el artículo 21 del Decreto 1377 de 2013 (Incorporado en el Decreto 1074 de 2015) desarrolló el mencionado derecho. De acuerdo con este, es

71 El artículo 11 de la Ley 1581 de 2012, establece que, "*La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos*".

deber de los Responsables establecer mecanismos sencillos y ágiles que estén permanentemente disponibles para los Titulares con el fin de que estos puedan acceder a los Datos personales que estén bajo el control de aquellos y, en dicho sentido, puedan ejercer sus derechos sobre los mismos.

Más aún, se le exige al Responsable permitir el acceso al Titular a su información, de manera gratuita: (i) al menos una (1) vez cada mes calendario, y (ii) cada vez que existan modificaciones sustanciales de las políticas de Tratamiento de información (en adelante PTI) que motiven nuevas consultas.

Cuando las consultas que requiera el Titular sean mayores a una (1) por cada mes calendario, el Responsable *“sólo podrá cobrar al titular los gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente”*<sup>72</sup>.

Por último, cabe mencionar que todos los procedimientos de acceso a la información deben darse a conocer y ser fácilmente accesibles a los Titulares de esta e incluirse en la PTI<sup>73</sup>.

## **2.2. Artículo 12 de la Ley 1581 de 2012**

La Autorización para el Tratamiento de los Datos personales es calificada. Lo anterior, por cuanto debe ser previa, expresa e informada. Bajo esta premisa, el artículo 12 de la Ley 1581 de 2012 le ordena a los Responsables del Tratamiento que al momento de solicitar al Titular dicha Autorización, se le informe de manera clara y expresa lo siguiente: el Tratamiento al cual serán sometidos sus Datos personales y la finalidad del mismo; el carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre Datos sensibles o sobre los Datos de las niñas, niños y adolescentes; los derechos que le asisten como Titular; y, la identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

Para cumplir lo que ordena el citado artículo, el Responsable debe satisfacer dos criterios: i) la información tiene que estar disponible al momento de solicitar al Titular la Autorización; y, ii) aquella debe ser informada de manera clara y expresa. Por lo tanto, solo se entenderá satisfecho el requisito de una Autorización informada cuando el Responsable del Tratamiento cumpla ambos criterios.

72 Artículo 21 del Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015).

73 Artículo 18 del Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015).

### 2.2.1. Datos sensibles

Se mencionó que debe informarse el carácter facultativo de la respuesta a las preguntas que le sean hechas al Titular, cuando estas versen sobre Datos sensibles. Al respecto, el artículo 6 del Decreto 1377 de 2013 adiciona a dicho deber lo siguiente: informarle al Titular cuáles de los Datos que serán objeto de Tratamiento son sensibles y la finalidad de este. Por último, el citado artículo ordena que ninguna actividad sea condicionada a que el Titular suministre Datos personales sensibles.

## 2.3. Política de Tratamiento de Información (PTI)

Mediante esta el deber de información se materializa en la regulación colombiana. Al respecto, es el Decreto 1377 de 2013 quien les ordena a los Responsables del Tratamiento desarrollar una PTI. Estas, a su vez, deberán constar en medios físicos o electrónicos; estar en un lenguaje claro y sencillo; y ser puestas en conocimiento de los Titulares.

El citado decreto exige que la PTI contenga, como mínimo, la siguiente información: 1) nombre o razón social; domicilio; dirección; correo electrónico y teléfono del Responsable; 2) Tratamiento al cual serán sometidos los Datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad; 3) derechos que le asisten como Titular; 4) persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el Titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el Dato y revocar la Autorización; 5) procedimiento para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la Autorización; y 6) fecha de entrada en vigencia de la política de Tratamiento de la información y período de vigencia de la Base de Datos.

### 2.3.1. Difusión de la PTI

El deber de información que se materializa con la PTI no se satisface con la mera redacción del documento. Lo anterior, toda vez que ésta deberá ser difundida por el Responsable y darla a conocer a través de documentos; formatos electrónicos; medios verbales o cualquier otra tecnología; siempre y cuando garantice y cumpla con el deber de informar al Titular<sup>74</sup>.

74 Artículo 17 del Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015).

### 2.3.2. Cambios en la PTI

Son cambios sustanciales en el contenido de la PTI, los siguientes: la identificación del Responsable; y la finalidad del Tratamiento de los Datos personales, debido a que, pueden afectar el contenido de la Autorización. Por lo tanto, es deber del Responsable comunicar estos cambios al Titular antes de o a más tardar al momento de implementar las nuevas políticas. Además, se le exige obtener del Titular una nueva Autorización cuando el cambio se refiera a la finalidad del Tratamiento.

Estas circunstancias se deberán comunicar a los Titulares oportunamente y de manera eficiente.

## 2.4. Registro Nacional de Bases de Datos

Otra forma como el principio de transparencia se materializa es en el Registro Nacional de Bases de Datos (RNBD). Éste es el directorio público de las Bases de Datos sujetas a Tratamiento que operan en el país<sup>75</sup>. Por su parte, el artículo 25 de la Ley 1581 de 2012 obliga a los Responsables aportar a la Superintendencia de Industria y Comercio las PTI para realizar el registro de Bases de Datos<sup>76</sup>. En adición, el citado artículo dispone que las PTI en ningún caso podrán ser inferiores a los deberes contenidos en la Ley 1581 de 2012.

Cualquier ciudadano puede consultar las bases de datos registradas por un Responsable del Tratamiento y conocer las PTI de cada Responsable. Lo anterior se puede realizar por medio digital en la página web de la Superintendencia de Industria y Comercio<sup>77</sup>.

## 2.5. Aviso de privacidad

Por último, la regulación obliga a los Responsables, en los casos en los que no sea posible poner a disposición la PTI, informar por medio de un aviso de privacidad

75 Los Responsables del Tratamiento no cargan sus bases de datos con información personal en el RNBD, solamente inscriben la información establecida en el Capítulo 26 del Decreto Único 1074 de 2015 y en la Circular Única de la Superintendencia de Industria y Comercio.

76 De acuerdo con el artículo 25 de la Ley 1581 de 2012, “El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país. El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos”.

77 Según información de la Superintendencia de Industria y Comercio publicada en <https://rnbd.sic.gov.co/sisi/consultaTitulares/consultas/> para el 6 de abril del 2022 el RNBD se había consultado 388008 veces.

(en adelante AP) al Titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los Datos personales<sup>78</sup>.

El AP deberá contener, por lo menos, la siguiente información: nombre o razón social y Datos de contacto del Responsable del Tratamiento; el Tratamiento al cual serán sometidos los datos y la finalidad de este; los derechos que le asisten al Titular; los mecanismos dispuestos por el Responsable para que el Titular conozca la PTI y los cambios sustanciales que se produzcan en ella o en el AP; informar al Titular cómo acceder o consultar la PTI<sup>79</sup>.

Se destaca que la divulgación del AP no exime al Responsable de la obligación de dar a conocer a los Titulares la PTI, de conformidad con lo establecido en el Decreto 1377 de 2013<sup>80</sup>.

En últimas, el principio de transparencia conlleva un deber de información por parte del Responsable para con el Titular. El deber de información, que subyace del principio de transparencia, pretende generar confianza en los procesos que afectan al Titular. De esta forma, le permitirá no sólo comprenderlos, sino también cuestionarlos<sup>81</sup>. Precisamente, el deber de información tiene como objetivo reducir la asimetría de información entre los Titulares y los Responsables del Tratamiento, nivelando el campo de juego<sup>82</sup>.

La legislación colombiana le exige al Responsable que la información relativa al Tratamiento no sea secreta para el Titular. Justamente porque el Titular necesita poder conocer quién y para qué tratará su información. Lo anterior con el fin de ejercer sus derechos fundamentales. En concordancia, la información sobre las *cookies* facilitada en el momento de solicitar la Autorización debe ser suficientemente completa para permitir a los Titulares entender sus finalidades y el uso que se les dará.

78 Artículo 14 del Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015).

79 Artículo 15 del Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015).

80 Artículo 15 del Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015).

81 Grupo de Trabajo del Artículo 29. Directrices sobre transparencia con arreglo al Reglamento 2016/679 del 11 de abril de 2019.

82 Como lo menciona Nelson Remolina Angarita, *“el principio de transparencia no consiste solo en el acceso a la información del titular, sino garantizarle claridad sobre aspectos relevantes en cuanto al Tratamiento y sus derechos, suministrándole información sobre, entre otros aspectos, sus prácticas y políticas en la materia”* En Tratamiento de Datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012 (LEGIS, Bogotá, 2013).

### III. Realidades y retos

El panorama da cuenta de las deficiencias que se han detectado por parte de las autoridades de protección de Datos, relativas al principio de transparencia. Lo anterior, demuestra que persisten retos para aquellos Responsables que utilizan *cookies* para recoger Datos personales en el ciberespacio<sup>83</sup>.

#### 1. Realidad

A continuación, se hará referencia a dos hipótesis en las que se vulnera el principio de transparencia, las cuales han sido identificadas por las autoridades de protección de Datos. En primer lugar, la obtención de la Autorización sin el lleno de requisitos legales. Y, en segundo lugar, la difusión de PTI ausentes de la información mínima requerida.

##### 1.1. Vulneración del artículo 12 de la Ley 1581 de 2012

Un Responsable del Tratamiento que utiliza *cookies* para tratar Datos personales puede vulnerar el principio de transparencia cuando no le informa al Titular todo lo que ordena el artículo 12 de la Ley Estatutaria 1581 de 2012. En Colombia, la Superintendencia de Industria y Comercio se ha pronunciado sobre este asunto en dos oportunidades<sup>84</sup>.

En primer lugar, mediante la Resolución 53593 del 3 de septiembre de 2020<sup>85</sup> concluyó que la compañía Google LLC incumple el cincuenta y ocho punto tres por-

83 El CONPES 3701 relativo a los Lineamientos de Política para Ciberseguridad y Ciberdefensa define ciberespacio como: “Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios”.

La recolección de Datos personales por medio de web *cookies* genera varios interrogantes jurídicos. Por esta razón, otros temas de investigación que no aborda el presente texto son, entre otros, los siguientes: i) las prácticas abusivas en la recolección de Datos personales por medio de web *cookies*; y, la vulneración a los deberes que emanan del principio de libertad.

84 Para determinar qué resoluciones de la Superintendencia de Industria y Comercio serían analizadas se optó por identificar aquellas que evaluaron el cumplimiento de los deberes que emanan del principio de transparencia. Así, el ámbito de aplicación de la norma o el domicilio de los Responsables no fue un factor de selección.

85 La Superintendencia de Industria y Comercio resolvió el recurso de apelación interpuesto por la sociedad Google LLC mediante Resolución N° 60478 del 21 de septiembre de 2021.

ciento (58,3%) de los requisitos exigidos por dicha norma; cumple correctamente el doce punto cinco por ciento (12,5%); y, parcialmente, el veintinueve punto dos por ciento (29,2%) de los mismos.

En segundo lugar, en la Resolución 62132 del 5 de octubre de 2020 encontró que la aplicación TikTok no cumple el cincuenta y ocho punto treinta y tres por ciento (58,33%) de los requisitos exigidos por la regulación colombiana respecto de lo que se le debe informar a las personas antes de obtener su Autorización para poder recolectar y usar sus Datos personales.

Nótese que un consentimiento que ha sido otorgado por un Titular al que no se le ha garantizado la información mínima requerida por el artículo 12 de la ley estatutaria, es a todas luces inválida. Así, sólo será legitimadora una Autorización que hubiere sido otorgada de manera previa, expresa y debidamente informada<sup>86</sup>.

Si bien no es materia de análisis del presente escrito, es importante considerar que en la recolección de Datos personales por medio de *cookies* surge la discusión respecto al *opt-in* y el *opt-out*. El primero hace referencia al proceso utilizado cuando se requiere una acción positiva por parte del Titular al momento de autorizar el uso de *cookies*. Mientras que el segundo se refiere a aquella situación en donde no se requiere que el Titular otorgue su Autorización de forma activa antes de configurar las *cookies*, sin embargo, se le debe dar a este la posibilidad de rechazarlas posteriormente.

Por su parte, la legislación colombiana establece los siguientes modos de obtener la Autorización: (i) por escrito; (ii) de forma oral; o (iii) mediante conductas inequívocas del Titular que permitan concluir de forma razonable que otorgó la Autorización. No obstante, en ningún caso el silencio podrá asimilarse a una conducta inequívoca<sup>87</sup>. Más aún, es deber del Responsable poner a disposición del Titular mecanismos gratuitos y de fácil acceso para presentar la solicitud de revocatoria de la Autorización otorgada<sup>88</sup>.

Entonces, una Autorización para el Tratamiento de Datos personales por medio de *cookies* será válida cuando, además de cumplir con los deberes de información establecidos en el artículo 12 de la Ley 1581 de 2012, sea previa y expresa en

86 Para que una Autorización se entienda debidamente informada se le debe haber comunicado al Titular al momento de solicitar la Autorización, como mínimo, aquello que establece el artículo 12 de la Ley 1581 de 2012.

87 Artículo 7 del Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015).

88 Artículo 9 del Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015).

concordancia con lo establecido en los artículos 7, 8 y 9 del Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015).

## 1.2. Vulneración a los deberes de información en la PTI

Un Responsable del Tratamiento que utiliza *cookies* para tratar Datos personales también puede vulnerar el deber de información cuando su PTI y/o el AP no cumplen los requisitos mínimos de ley. Trayendo a colación los casos previamente analizados, se extraen las siguientes conclusiones.

Primero, la Resolución 62132 del 5 de octubre de 2020<sup>89</sup>, concluyó que de los diez y nueve (19) ítems que se evaluaron de la PTI de la aplicación TikTok ésta: cumple correctamente nueve (47,37%); cumple parcialmente uno (5,26%); y no cumple nueve (47,37%)<sup>90</sup>.

Segundo, al revisar la PTI de la compañía Google LLC la autoridad concluyó que aquel cumple correctamente cuatro (21,05%); cumple parcialmente cinco (26,31%); y no cumplen diez (52,63%)<sup>91</sup> de los ítems evaluados.

En este sentido, son varias las autoridades de protección de Datos personales que han identificado una vulneración al deber de información en la recolección de Datos personales por medio de *cookies*. En la siguiente tabla se exponen algunos de los hallazgos de estas autoridades<sup>92</sup>.

89 La Superintendencia de Industria y Comercio resolvió el recurso de apelación interpuesto por la sociedad TikTok Inc. mediante Resolución N° 67413 del 19 de octubre de 2021.

90 Superintendencia de Industria y Comercio, Resolución N° 62132 del 5 de octubre de 2020 (Por medio de la cual se emiten ordenes administrativas a las sociedades ByteDance Ltd., TikTok, Inc. y TikTok Pte. Ltd.). Los recursos de apelación interpuestos por las sociedades ByteDance Ltd. y TikTok Pte. Ltd. fueron resueltos mediante la Resolución N° 75009 del 22 de noviembre de 2021 y la Resolución 75008 del 22 de noviembre de 2021 respectivamente.

91 Superintendencia de Industria y Comercio, Resolución N° 53593 del 3 de septiembre de 2020 (Por medio de la cual se emiten ordenes administrativas a la sociedad Google LLC).

92 El Tribunal de Justicia Europeo también se ha pronunciado al respecto. En sentencia con asunto C-673/17 en el procedimiento entre Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV y Planet49 GmbH, expresó que, “Si bien el tiempo durante el cual se va a proceder al Tratamiento de los datos no se halla entre dichas indicaciones, de la expresión «por lo menos» que figura en el artículo 10 de la Directiva 95/46 resulta, no obstante, que esta enumeración no es exhaustiva. Pues bien, debe considerarse que la información relativa al tiempo durante el cual las *cookies* estarán activas responde a la exigencia, establecida en dicho artículo, de que el Tratamiento de los datos sea leal, puesto que, en una situación como la controvertida en el litigio principal, un período de tiempo largo, o incluso ilimitado, implica la recogida de numerosos datos sobre los hábitos de navegación y la frecuencia de las eventuales visitas del usuario a los sitios de los socios publicitarios del organizador del juego con fines promocionales. Esta interpretación queda corroborada por el artículo 13, apartado 2, letra a), del Reglamento 2016/679, que prevé que, para garantizar un Tratamiento de datos leal y transparente, el responsable del Tratamiento debe facilitar al interesado información, entre otras cosas, sobre el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, sobre los criterios utilizados para determinar este plazo”.

Autoridad de Protección de Datos Personales	Decisión	Resumen
Comisión Nacional de Informática y de las Libertades (CNIL)	Decisión SAN -2020-012 de diciembre 7 de 2020 relativa a Google LLC y Google Ireland Limited	<p>“Cuando un usuario visitaba la página google.fr, se mostraba un banner de información en la parte inferior de la página, con la siguiente nota “Recordatorio de privacidad de Google”, frente a la cual había dos botones: “Recordarme más tarde” y “Acceder ahora”.</p> <p>Este banner no proporcionó al usuario ninguna información sobre las cookies que, sin embargo, ya se habían colocado en su computadora al ingresar al sitio. La información tampoco se proporcionó cuando hizo clic en el botón “Acceder ahora””.</p>
Comisión Nacional de Informática y de las Libertades (CNIL)	Decisión SAN-2020-013 de 17 de diciembre de 2020 relativa a Amazon Europe Core	<p>“Primero, el comité señaló que, en el caso de un usuario que visita el sitio web amazon.fr, la información proporcionada no era clara ni completa.</p> <p>Consideró que el banner informativo desplegado por la empresa, que era “Al utilizar este sitio web, acepta nuestro uso de cookies permitiendo ofrecer y mejorar nuestros servicios. Leer más.”, Solo contenía información general y aproximada sobre los propósitos de todas las cookies colocadas. En particular, consideró que, al leer el banner, el usuario no podía entender que las cookies colocadas en su equipo se utilizaban principalmente para mostrar anuncios personalizados. También señaló que el banner no explicaba al usuario que podía rechazar estas cookies y cómo hacerlo”.</p>
Agencia Española de Protección de Datos (AEPD)	Resolución r/00283/2020 de terminación del procedimiento por pago voluntario	<p>“El banner sobre cookies que se despliega al acceder a las páginas, proporciona información poco concisa o inteligible. Al utilizar expresiones como, “(...) para mejorar su navegación (...)”, inducen a confusión, desvirtuando la claridad del mensaje (punto 3.1.2.1 de la guía). Según el punto 3.1.2.2. de la guía, la información que debe proporcionarse en esta capa es una identificación genérica de las finalidades de las cookies que se utilizarán, como, por ejemplo: “utilizamos cookies para hacer perfiles basados en la navegación de los usuarios” o, “conocer el comportamiento del usuario mediante el análisis de su navegación con fines publicitarios””.</p>
Agencia Española de Protección de Datos (AEPD)	Resolución del Recurso de Reposición No-RR/582/2020 (Caso Iberia)	<p>“(…) la falta de información sobre la correcta identificación de la cookies propia y de terceros (tiempo que permanecen activas e instaladas en el equipo terminal), no ha sido hasta la presentación de este recurso de reposición, cuando la entidad ha subsanado esta deficiencia, once meses después de haber asegurado que su página web cumplía fielmente lo estipulado en la normativa vigente en materia de protección de datos y en las recomendaciones hechas por esta Agencia en su “guía sobre cookies”, (...)”.</p>

Tabla 4. Decisiones de Autoridades de Protección de Datos en Europa sobre infracciones al deber de información en el uso de *cookies*

Elaborada por el autor.

En adición, se pone de presente que actualmente existen prácticas en las que se posibilita “omitir” las preferencias del Titular en la configuración del navegador<sup>93</sup>. En otras palabras, se ignoran los deseos de este. Estas prácticas no solo son contrarias al ordenamiento jurídico colombiano, también son abusivas.

Así pues, actuar en contra de las preferencias preseleccionadas por el Titular<sup>94</sup>, además de abusivo, es contrario al principio de transparencia. Pues, implica que el Titular no esté informado sobre las circunstancias que rodean la instalación y el uso de *cookies* y, por consiguiente, el Tratamiento de su información.

## 2. Retos

El uso de *cookies* es compatible con un debido Tratamiento de Datos personales. Por tanto, el desafío de las organizaciones que emplean esta tecnología es hacerlo bien desde el principio. Para lograrlo, las organizaciones deberían: i) implementar estrategias de Responsabilidad Demostrada frente al Tratamiento de Datos personales; e ii) implementar el principio de privacidad desde el diseño y por defecto.

### 2.1. Principio de Responsabilidad Demostrada (Accountability)

Desde un principio el Responsable debe establecer una estrategia para probar que ha adoptado las medidas útiles para cumplir las normas sobre el Tratamiento de Datos personales. Lo anterior, toda vez que *“Los Responsables del Tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012”*<sup>95</sup>.

La Corte Constitucional, en Sentencia C-032 del 2021 afirmó que,

“El principio de responsabilidad demostrada, de acuerdo con lo expuesto, consiste en el deber jurídico del responsable del Tratamiento de demostrar ante la autoridad

93 Kost, “Peeking into the cookie jar”, 394.

94 Las denominadas flash *cookies*, no se controlan a través de los navegadores y permiten que las *cookies* “reaparezcan”. Dichas cookies no se ven afectadas por ninguna solución relacionada con las mejoras de privacidad de la configuración del navegador.

95 Artículo 26 del Decreto 1377 de 2013 (Incorporado en el Decreto 1074 de 2015).

Medidas “apropiadas” son aquellas ajustadas a las necesidades del Tratamiento de datos. Y “efectivas” son aquellas que permiten lograr el resultado o efecto que se desea o espera.

de datos que cuenta con la institucionalidad y los procedimientos para garantizar las distintas garantías del derecho al habeas data, en especial, la vigencia del principio de libertad y las facultades de conocimiento, actualización y rectificación del dato personal”.

Por su parte, la Superintendencia de Industria y Comercio en múltiples pronunciamientos se ha referido a la responsabilidad de los administradores. Al respecto, afirma que,

“(…) los administradores deben cuidar al detalle y con perfecta seguridad este aspecto. No basta solo con ser guardianes, deben ser promotores de la correcta y precisa aplicación de la ley. Esto, desde luego, los obliga a verificar permanentemente si la ley se está o no cumpliendo en todas las actividades que realiza su empresa u organización”<sup>96</sup>.

Por esta razón, no se puede perder de vista que, en el contexto de nuevas tecnologías, quienes recolectan información deben actuar de manera proactiva como administradores Responsables y éticos de los Datos personales.

Si los Responsables del Tratamiento no actúan de manera proactiva, responsable y ética, los ciudadanos digitales no sabrán qué se está haciendo con su información y quién tiene información sobre ellos. Lo cual les impide ejercer un control eficiente y certero sobre sus Datos.

## 2.2. Privacidad desde el diseño y por defecto

La privacidad desde el diseño y por defecto<sup>97</sup> es considerada una medida proactiva para, entre otras, cumplir con el principio de Responsabilidad Demostrada. Así, la mejor manera de garantizar el debido Tratamiento de datos es tomando la privacidad como un componente esencial desde el diseño y puesta en marcha del producto o servicio. La Privacidad por Diseño “*promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios;*

96 Superintendencia de Industria y Comercio, Resolución N° 38281 del 14 de julio de 2020.

97 La Autoridad Española de Protección de Datos, afirma lo siguiente sobre la restricción por defecto, “*El caso de uso que, siendo lo más restrictivo por defecto, permita acceder a la funcionalidad básica del sistema (funcionalidad inicial, valores de fábrica) siempre ha de estar disponible y seleccionado inicialmente sin necesidad de ningún cambio por parte del responsable o del usuario*”. “Guía de Protección de Datos”, Agencia Española de Protección de Datos, acceso el 10 de abril de 2021, <https://www.aepd.es/es/documento/guia-proteccion-datos-por-defecto.pdf>

*más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización*<sup>98</sup>.

Con ese objetivo, se debe propender por facilitar a los usuarios información clara y completa sobre la utilización de los dispositivos de almacenamiento y recuperación de Datos. Y, en particular, sobre los fines del Tratamiento de los Datos recolectados<sup>99</sup>. Esta información debe facilitarse, como se ha indicado, con arreglo a lo dispuesto en la legislación colombiana en la materia. La cual indica que el Tratamiento de los Datos de los usuarios se deberá realizar de forma transparente hacia ellos.

En Colombia está prohibido utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales<sup>100</sup>. Esto le impone al Responsable la obligación previa de determinar quiénes son los Titulares a los que se dirigirá y qué se supone deben encontrar inteligible y de fácil acceso<sup>101</sup>. En palabras de la Superintendencia de Industria y Comercio,

“El requisito de que el lenguaje sea claro y sencillo significa que, por ejemplo, la política sea comprensible para el tipo de audiencia; esto reviste especial importancia cuando se trata de niños, niñas o adolescentes, o personas con alguna discapacidad, o personas de la tercera edad, o personas que no hablen el idioma empleando en la redacción”<sup>102</sup>.

El principio de transparencia no pretende que los Titulares se “inmiscuyan” en el flujo de Datos o en los algoritmos que los mueven. Es decir, no se trata de revelar ninguna práctica protegida legalmente o un secreto empresarial. Sino que, busca proporcionar una determinada narrativa que se construya, adapte y ajuste a

98 “Privacidad por Diseño: Los 7 principios fundamentales”, Ann Cavoukian, acceso el 5 de abril de 2021, <https://www.mediascope.es/wp-content/uploads/2016/10/privacidad-por-disen%CC%83o-1.pdf>.

99 Informar a los Titulares no es algo nuevo en internet. Quienes crean contenido en el mundo digital saben qué métodos utilizar para atraer la atención de los Titulares hacia aquella información que desean resaltar, como en el caso de promociones, ofertas o encuestas de satisfacción. Así, debería aprovecharse la experiencia adquirida para aquellos fines con el propósito de obtener la Autorización informada de los Titulares.

100 Inciso 3 del Artículo 4 del Decreto 1377 de 2013 (Incorporado en el Decreto 1074 de 2015).

101 Aquella narrativa construida especialmente para los Titulares debe ajustarse a una determinada idea de las presuntas necesidades y capacidades de discernimiento del lector (el Titular). Entonces, la información debe transmitirse de una manera objetivamente concisa y usando un lenguaje claro y sencillo, pero también de una manera que se adapte subjetiva y contextualmente a la capacidad de los Titulares para entender su significado y darle algún sentido.

102 Superintendencia de Industria y Comercio, Resolución N° 53593 del 3 de septiembre de 2020 (Por medio de la cual se emiten ordenes administrativas a la sociedad Google LLC).

las necesidades y capacidades del Titular en cuanto al conocimiento de las actividades que se realicen sobre su información<sup>103</sup>.

En resumen, la información sobre las *cookies* facilitada en el momento de solicitar la Autorización debe ser suficientemente completa para permitir a los Titulares entender sus finalidades y el uso que se les dará. Es de recordarse que cuando existe confianza, la persona cree que la empresa es fiable; cumple sus políticas; es sincera; íntegra, y lleva a cabo las acciones prometidas. Así, una organización transparente puede generar mayor confianza en sus clientes y en los Titulares de los Datos<sup>104</sup>.

## Conclusiones

La regulación sobre Tratamiento de Datos personales debe aplicarse al margen de los procedimientos, metodologías o tecnologías que se utilicen para recolectar, usar o tratar ese tipo de información. Toda vez que una *cookie* es un mecanismo que se instala en los equipos de los Titulares de la información con el objetivo de recolectar algunos de sus Datos personales, dicho Tratamiento está sujeto a las disposiciones de la Ley 1581 de 2012 y sus decretos reglamentarios.

Para responder la pregunta de investigación fue necesario identificar los deberes que emanan del principio de transparencia. En primer lugar, se identificó la exigencia para que toda la información relativa al Tratamiento de los Datos personales sea fácilmente accesible y de simple entendimiento. Más aún, se determinó que en la legislación nacional el principio de transparencia se materializa en cinco pilares<sup>105</sup>.

Como se mencionó, en Colombia la regulación proscribe utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales. En este sentido, utilizar *cookies* sin cumplir con todos los deberes que emanan del principio de transparencia es un ejemplo de recolección por medios engañosos y fraudulentos.

103 Como parte de la información sobre *cookies*, se recomienda que el Responsable le comunique al Titular, por lo menos, lo siguiente: la definición y función genérica de la tecnología *cookie*; información sobre el tipo de *cookie* que se utilizan y su finalidad; identificación de quién utiliza las *cookies*. Esto es, quiénes son todos los Responsables del Tratamiento; información sobre la forma de aceptar, denegar o revocar el consentimiento para el uso de *cookies*; información sobre las transferencias de Datos a terceros países; periodo de conservación de los Datos; y la demás información requerida por ley.

104 “Guía sobre el Tratamiento de Datos personales para fines de comercio electrónico”, Superintendencia de Industria y Comercio, acceso el 19 de marzo de 2021, [https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico(1).pdf)

105 Como se indicó, los cinco pilares son: i) el Derecho de acceso; ii) el artículo 12 de la Ley 1581 de 2012; iii) la PTI; iv) el AP; y, v) el RNBD.

Es por lo anterior que reviste de gran importancia que las organizaciones que emplean esta tecnología hagan bien las cosas desde el comienzo. Si logran esto, los Responsables del Tratamiento de Datos personales que usan web *cookies* para su recolección evitan vulnerar los deberes que emanan del principio de transparencia, a saber: 1) informar lo dispuesto en el artículo 12 de la Ley 1581 de 2012; 2) poner a disposición del público la PTI y el AP en consonancia con los requisitos legales; 3) registrar en el RNBD la PTI; y, 3) permitir el acceso a los Titulares de su información.

Para lograr esto, entre otras, es indispensable implementar estrategias de Responsabilidad Demostrada frente al Tratamiento de Datos personales; e implementar el principio de privacidad desde el diseño y por defecto.

Con eso en mente, se debe facilitar a los Titulares información clara y completa sobre la utilización de *cookies*. Y, en particular, sobre los fines del Tratamiento de los Datos recolectados. Esta información debe facilitarse, como se ha indicado, con arreglo a lo dispuesto en la legislación colombiana en la materia. La cual indica que el Tratamiento de los Datos de los usuarios se deberá realizar de forma transparente hacia ellos desde el comienzo.

Ahora bien, la Responsabilidad Demostrada exige adoptar medidas apropiadas y útiles. Por eso, de manera proactiva el Responsable podría indicarle al Titular lo siguiente:

- La definición y función genérica de la tecnología *cookie*.
- Información sobre el tipo de *cookies* que se utilizan y sus finalidades.
- Identificación de quién utiliza las *cookies*. Esto es, quienes son todos los Responsables del Tratamiento.
- Información sobre la forma de aceptar, denegar o revocar la Autorización para el uso de *cookies*.
- Información sobre las transferencias de Datos a terceros países.
- Periodo de conservación de los Datos.
- La demás información requerida por ley.

Para concluir, toda la información que se le brinde al Titular sobre las *cookies* debe ser suficientemente completa para que este entienda las finalidades y el uso que se le dará a sus Datos personales. Cuando existe confianza, la persona cree que la empresa es fiable; cumple sus políticas; es sincera; integra, y lleva a cabo las acciones prometidas. Así, una organización transparente puede generar mayor confianza en los Titulares de la información.

## Referencias

Agudelo Giraldo, Óscar Alexis. La pregunta por el método: derecho y metodología de la investigación. Bogotá: Editorial Universidad Católica de Colombia, 2018.

Al-Rousan, Thamer. "An Investigation of User Privacy and Data Protection on User-Side Storages". *International Journal of Online and Biomedical Engineering* 15, n° 9 (2019): 17-30, <https://doi.org/10.3991/ijoe.v15i09.10669>.

Bennett, Collin. "Cookies, web bugs, webcams and cue cats: Patterns of surveillance on the world wide web". *Ethics and Information Technology* 3, n° 3 (2001): 197-210, <https://doi.org/10.1023/A:1012235815384>.

Berghel, Hal. "Digital Village: Caustic cookies". *Communications of the ACM* 44, n° 5 (2001): 19-22, <https://doi.org/10.1145/374308.374320>.

Bygrave, Lee. *Data Protection Law: Approching its Rationale, Logic and Limits*. Londres: Kluwer Law International, 2000.

Comisión Nacional de Informática y de las Libertades (CNIL) de la República Francesa. Decisión N° SAN -2020-012 de diciembre 7 de 2020 relativa a Google LLC y Google Ireland Limited.

Comisión Nacional de Informática y de las Libertades (CNIL) de la República Francesa. Decisión N°SAN-2020-013 del 17 de diciembre de 2020 relativa a Amazon Europe Core.

Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Resolución de Madrid. Estándares Internacionales sobre Protección de Datos Personales y Privacidad. 5 de noviembre de 2009 en Madrid.

Consejo de Europa. Convenio 108 del 28 de enero de 1981, para la protección de las personas respecto al Tratamiento automatizado de datos de carácter personal.

Consejo de Europa. Convenio 108+ de junio de 2018, para la protección de las personas respecto al Tratamiento automatizado de datos de carácter personal.

Constitución Política de Colombia. Gaceta Constitucional número 114 del 4 de julio de 1991.

"Cookie sweep combined analysis report". Grupo de Trabajo del artículo 29, [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwicwNOpksztAhXmQd8KHfQPbClQFjABegQIA RAC&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fdocument.cfm%3Faction%3Ddisplay%26doc\\_id%3D56123&usg=AOvVaw1GeyzU33CSutUzfCODzNbF](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwicwNOpksztAhXmQd8KHfQPbClQFjABegQIA RAC&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fdocument.cfm%3Faction%3Ddisplay%26doc_id%3D56123&usg=AOvVaw1GeyzU33CSutUzfCODzNbF)

Corte Constitucional, Sentencia C-032 del 18 de febrero de 2021. M.P. Gloria Stella Ortiz Delgado.

Corte Constitucional, Sentencia C-1147 del 31 de octubre de 2011. M.P. Manuel José Cepeda Espinosa.

Corte Constitucional, Sentencia C-640 del 18 de agosto de 2010. M.P. Mauricio González Cuervo.

Corte Constitucional, Sentencia C-748 del 6 de octubre de 2011. M.P. Jorge Ignacio Pretelt Chaljub.

Corte Constitucional, Sentencia T-414 del 16 de junio de 1992. M.P. Ciro Angarita Barón.

Corte Constitucional, Sentencia T-509 del 9 de diciembre de 2020. M.P. José Fernando Reyes Cuartas.

Decreto 1377 de 2013, 27 de junio. Diario Oficial N° 48834.

Decreto Reglamentario 1074 de 2015, 26 de mayo. Diario Oficial No. 49523

Departamento Nacional de Planeación. Documento CONPES 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa.

Departamento Nacional de Planeación. Documento CONPES 4012 Política Nacional de Comercio Electrónico.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002. Diario Oficial de las Comunidades Europeas 31.7.2002.

Domínguez, Ana Garriga. Nuevos retos para la protección de datos personales: en la era del Big Data y de la computación ubicua. Madrid: Dykinson, 2016.

Drury, Alexandra. "How Internet User's Identities Are Being Tracked and Used". Tulane Journal of Technology and Intellectual Property 15 (2012): 219-241, [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjrvJSO3P32AhWASTABHUcJBoMQFnoECAkQAQ&url=https%3A%2F%2Fjournals.tulane.edu%2FTIP%2Farticle%2Fview%2F2613%2F2435&usq=AOvVaw0Cavq5Ow\\_semk61MjRVYAm](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjrvJSO3P32AhWASTABHUcJBoMQFnoECAkQAQ&url=https%3A%2F%2Fjournals.tulane.edu%2FTIP%2Farticle%2Fview%2F2613%2F2435&usq=AOvVaw0Cavq5Ow_semk61MjRVYAm).

Formato modelo para el cumplimiento de obligaciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios, Superintendencia de Industria y Comercio, [https://www.sic.gov.co/sites/default/files/files/Nuestra\\_Entidad/Publicaciones/Cartilla\\_formatos\\_datos\\_Personales\\_nov22.pdf](https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_formatos_datos_Personales_nov22.pdf)

Foro de Cooperación Económica Asia Pacífico. Marco de Privacidad, 2004.

González Fuster, Gloria. "Transparency As Translation In Data Protection". En Being Profiled: Cogitas Ergo Sum: 10 Years Of Profiling The European Citizen, coordinado por Bayamlioğlu Emre y Baraliuc Irina. Amsterdam: Amsterdam University Press, 2018, 52-57.

González Guerrero, Daniela. “Control De Nuestros Datos Personales En La Era Del Big Data: El Caso Del Rastreo Web De Terceros”, *Estudios Socio-Jurídicos* 21, n° 1 (2019): 209-244, <https://doi.org/10.12804/revistas.urosario.edu.co/sociojuridicos/a.6941>.

Grupo de Trabajo del Artículo 29. Dictamen 1/2009 sobre las propuestas de modificación de la Directiva 2002/58 / CE sobre privacidad y comunicaciones electrónicas.

Grupo de Trabajo del Artículo 29. Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679. Adoptadas el 4 de mayo de 2020.

Grupo de Trabajo del Artículo 29. Directrices sobre transparencia con arreglo al Reglamento 2016/679. Adoptadas 11 de abril de 2019.

“Guía para la gestión de incidentes de seguridad en el Tratamiento de Datos personales”. Superintendencia de Industria y Comercio, [https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia\\_gestion\\_incidentes\\_dic21\\_2020.pdf](https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf)

“Guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de Datos personales”. Superintendencia de Industria y Comercio, [https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales(1).pdf)

“Guía para la implementación del principio de responsabilidad demostrada (Accountability)”. Superintendencia de Industria y Comercio, <https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

“Guía sobre Cookies y otras tecnologías de seguimiento”. Comisión de Protección de Datos de la República de Irlanda, <https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf>

“Guía sobre el Tratamiento de Datos personales para fines de comercio electrónico”. Superintendencia de Industria y Comercio, [https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico(1).pdf)

“Guía sobre el Tratamiento de Datos personales para fines de marketing y publicidad”. Superintendencia de Industria y Comercio, <https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20marketing%20y%20publicidad%20y%20Tratamiento%20de%20datos%202019.pdf>

“Guía sobre el Tratamiento de las fotos como Datos personales”. Superintendencia de Industria y Comercio, [https://www.sic.gov.co/sites/default/files/files/Publicaciones/Gu%C3%ADa%20Tratamiento%20de%20datos%20fotos%20FINAL%202014%20diciembre\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/Publicaciones/Gu%C3%ADa%20Tratamiento%20de%20datos%20fotos%20FINAL%202014%20diciembre(1).pdf)

“Guía sobre el uso de las cookies”. Agencia Española de Protección de Datos, <https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf>

“ICO, CNIL, German and Spanish DPA revised cookies guidelines: Convergence and divergence”. International Association of Privacy Professionals, [https://iapp.org/media/pdf/resource\\_center/CNIL\\_ICO\\_chart.pdf](https://iapp.org/media/pdf/resource_center/CNIL_ICO_chart.pdf)

Kost, Eleni. “Peeking into the cookie jar: the European approach towards the regulation of cookies”. *International Journal of Law and Information Technology*, 21, n° 4 (2013): 380-406, <http://dx.doi.org/10.2139/ssrn.2675810>.

Ley Estatutaria 1581 de 2012, 18 de octubre. Diario Oficial 48.587.

McCarthy, Laura y Yates, Dave. “The use of cookies in Federal agency web sites: Privacy and recordkeeping issues”. *Government Information Quarterly* 27, n° 3 (2010): 231-237, <http://www.sciencedirect.com/science/article/pii/S0740624X10000274>.

Newman, Joseph. “Cookie Monsters: Locally Stored Objects, User Privacy, and Section 1201 of the DMCA”. *AIPLA Quarterly Journal* 41, no. 3 (2013): 511-552.

Newman, Vivian y Ángel, María Paula. *Festín de datos Empresas y datos personales en América Latina*. Bogotá: Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia, 2020.

Organización de los Estados Americanos. *Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales*. Abril de 2021.

Organización para la Cooperación y el Desarrollo Económico. *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*. 2013.

Recomendaciones Generales para el Tratamiento de Datos en la inteligencia Artificial, Red Iberoamericana de Protección de Datos, [https://www.sic.gov.co/sites/default/files/files/pdf/1%20RIPD%20\(2019\)%20RECOMENDACIONES%20GENERALES%20PARA%20EL%20TRATAMIENTO%20DE%20DATOS%20EN%20LA%20IA.pdf](https://www.sic.gov.co/sites/default/files/files/pdf/1%20RIPD%20(2019)%20RECOMENDACIONES%20GENERALES%20PARA%20EL%20TRATAMIENTO%20DE%20DATOS%20EN%20LA%20IA.pdf)

Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016. Diario Oficial de la Unión Europea 4.5.2016.

Reigada, Antonio Troncoso. *La Protección de Datos Personales. En Busca del Equilibrio*. Valencia: Tirant lo Blanch, 2010.

Reino de España. Agencia Española de Protección de Datos (AEPD). Resolución r/00283/2020 de terminación del procedimiento por pago voluntario.

Reino de España. Agencia Española de Protección de Datos. Resolución del Recurso de Reposición No- RR/582/2020.

Remolina Angarita, Nelson. Recolección internacional de datos personales: un reto del mundo post-internet. Madrid: Agencia Española de Protección de Datos, 2015.

Remolina Angarita, Nelson. Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012. Bogotá: LEGIS, 2013.

Rodríguez, Juan Francisco. Figuras y responsabilidades en el Tratamiento de datos personales. Barcelona: BOSCH EDITOR, 2019.

Superintendencia de Industria y Comercio, “Respuesta a Consulta sobre *Web Cookies*”, Radicado 16-172268- -00001-0000.

Superintendencia de Industria y Comercio, Resolución N° 12192 del 1 de abril de 2020 (Resuelve recurso de apelación de la sociedad Facebook Inc.).

Superintendencia de Industria y Comercio, Resolución N° 38281 del 14 de julio de 2020 (Resuelve recurso de apelación de la sociedad Mervicol S.A.S.).

Superintendencia de Industria y Comercio, Resolución N° 53593 del 3 de septiembre de 2020 (Por medio de la cual se emiten ordenes administrativas a la sociedad Google LLC).

Superintendencia de Industria y Comercio, Resolución N° 59876 del 28 de septiembre de 2020 (Por medio de la cual se resuelve recurso de apelación de las sociedades Uber Technologies, Inc., Uber Colombia S.A.S. y Uber B.V).

Superintendencia de Industria y Comercio, Resolución N° 62132 del 5 de octubre de 2020 (Por medio de la cual se emiten ordenes administrativas a las sociedades ByteDance Ltd., TikTok, Inc. y TikTok Pte. Ltd.).

Superintendencia de Industria y Comercio, Resolución N° 74828 del 17 de diciembre de 2019 (Resuelve recurso de apelación de la sociedad Rappi S.A.S.).

Tribunal de Justicia Europeo (Gran Sala), sentencia con asunto C-673/17 del 1 de octubre de 2019.

Yue, Chuan y Xie, Mengjun. “An automatic HTTP cookie management system”. *Computer Networks*, Estados Unidos de America 54, n° 13 (2010): 2182–2198, <https://doi.org/10.1016/j.comnet.2010.03.006>.

Zuiderveen, Frederik. *Improving Privacy Protection in the Area of Behavioural Targeting*. Amsterdam: Wolters Kluwer, 2015.