ISSN 1794-5216

ANÁLISIS DEL PROCESO SANCIONATORIO DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS CONTRA FACEBOOK INC. (RESOLUCIÓN R/01870/2017), BAJO LA ÓPTICA DE LA NORMATIVA COLOMBIANA ACERCA DE LA PROTECCIÓN DE DATOS PERSONALES*

ANALYSIS OF THE SANCTIONS IMPOSED BY AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS AGAINST FACEBOOK INC. (RESOLUTION R/01870/2017), UNDER THE OPTIC OF COLOMBIAN LAW OF PERSONAL DATA

Diego Alejandro Cárdenas Gallagher**

Fecha de recepción: 25 de marzo de 2018
Fecha de aceptación: 3 de abril de 2018
Disponible en línea: 30 de julio de 2018

RESUMEN

El presente trabajo realiza un análisis de la Resolución R/01870/2017 emitida por la Agencia Española de Protección de Datos Personales en virtud de la cual sanciona a Facebook Inc. Por haber cometido múltiples violaciones a las normativas relativas a la protección

* El presente artículo fue producto del semillero de investigación en materia de competencia de la Pontificia Universidad Javeriana. Al profesor Carlos Andrés Uribe le transmito mi más profundo agradecimiento.

** Estudiante séptimo semestre de la Facultad de Derecho – Pontificia Universidad Javeriana. Bogotá, Colombia. Contacto: diegocardenas@javeriana.edu.co.

de datos personales. A raíz de este análisis se genera un ejercicio comparativo en relación con el ordenamiento jurídico colombiano y se muestran las semejanzas y diferencias entre ambos. Todo esto con el fin de mostrar el poco desarrollo práctico que ha tenido la normativa colombiana acerca de la protección de datos personales y las profundas preguntas que derivan de esto.

Palabras clave: Datos personales; *cookies*; *two-sided markets*; responsable del tratamiento; encargado del tratamiento.

ABSTRACT

This paper makes an analysis of the Resolution R/01870/2017 made by the *Agencia Española de Protección de Datos Personales* in which they sanctioned Facebook Inc. for violating several personal data laws. Furthermore, this paper makes a comparative exercise in relation with the colombian laws and shows the similarities and differences between them. All this with the purpose of showing the low practical development of the colombian law on this subject and the profound questions this generates.

Key words: Personal Data, cookies, two-sided markets, responsable of treatment, in charge of treatment.

INTRODUCCIÓN: DATOS PERSONALES, EL PRINCIPAL ACTIVO DEL MERCADO

Irónicamente días antes de presentar el siguiente artículo, Facebook sufrió una pérdida de más de 50 billones de dólares en Wall Street, por las filtraciones del uso indebido de la información de datos personales en las elecciones de Estados Unidos del año 2016[1]. Era cuestión de tiempo para darse cuenta que Facebook es la caja de pandora de nuestra época. Ojalá este artículo genere un aporte a este debate que acaba de volverse mundial.

A comienzos del siglo XX, Standard Oil Company era la empresa con mayor poder de mercado en el mundo. La mítica empresa creada por John D. Rocke-

1 Wall Street starts to trim Facebook targets as shares fall. https://www.reuters.com/article/us-facebook-stocks/wall-street-starts-to-trim-facebook-targets-as-shares-fall-idUSKBN1GX1MI. (Marzo 21 del 2018).

feller dominaba principalmente el mercado americano, chino y todas las zonas del Medio Oriente. Un siglo después, el petróleo ya no es el principal activo del mercado, la macro información digital a tomado la punta y la escasa regulación al respecto resulta preocupante. En mayo del año 2017, la revista *The Economist* publicó un provocador artículo titulado "*The world´s most valuable asset is no longer oil but data*"[2], en donde explica con mucho más detalle y acierto lo antes planteado. Sabiendo la relevancia actual —tanto económica como política— de los datos personales, el presente escrito busca mostrar cómo funciona la regulación de esta materia en Colombia. Lo anterior, usando un método de análisis comparado con un caso llevado a cabo por La Agencia Española de Protección de Datos en contra de Facebook Inc. En el año 2017, la Agencia Española de Protección de Datos Personales emitió la Resolución R/01870/2017, la cual contiene un proceso sancionatorio en contra de Facebook Inc. En virtud de esta resolución, Facebook Inc. fue sancionado por 1.200.000 euros, por múltiples incumplimientos de acuerdo con la Ley Española de Protección de Datos-Ley Orgánica 5 de 1992. De acuerdo con lo anterior, el presente escrito busca hacer un ejercicio comparativo, en virtud del cual, se tomen los hechos presupuestos en la resolución R/01870/2017 de la Agencia Española de Protección de Datos Personales y se miren a la luz de la legislación colombiana relativa a este tema. Lo anterior con el fin de intentar llegar a unas conclusiones que nos puedan hacer mejorar nuestras instituciones, autoridades, regulaciones y reglamentaciones relativas a la protección de datos personales. Todo esto, teniendo en consideración que se tratan de dos ordenamientos jurídicos diferentes y que generar un trasplante legal exacto puede terminar siendo contraproducente.

El presente escrito llevará el siguiente orden: primero, se hará una introducción al mundo de los datos personales y su relevancia actual. Segundo, se harán concisos comentarios acerca de la historia —en materia de datos personales— en Colombia. Tercero, se hará un breve recuento de los principales acontecimientos europeos en relación con el tema tratado. A renglón seguido, se empezará a desarrollar el caso concreto, Resolución R/01870/2017.

1. CONTEXTO GENERAL: EL MUNDO DE LOS DATOS PERSONALES

Los datos personales son definidos por nuestra legislación como: "…*cualquier información vinculada o que pueda asociarse a una o varias personas natura-*

2 The world's most valuable resource is no longer oil, but data. https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource. (Mayo 6 del 2017).

les determinadas o determinables"[3]. En otras palabras, es una información que genera una asociación a un ser humano. Lo importante a saber es que cuando se tiene la capacidad de recolectar la información de diversas personas, se forman bases estadísticas de las cuales se pueden hacer varias conclusiones comerciales, políticas, científicas, etc. El presente artículo centra principalmente su análisis sobre la finalidad comercial de los datos personales.

Cabe explicar la doble finalidad usada por las compañías con la macro información digital. En primer lugar, la información acerca de los usuarios es moldeada dentro de patrones que luego es vendida con fines publicitarios. Por ejemplo, si determinados usuarios en un rango de edad *x* muestran una interacción (ya sea a través de *me gusta* o *favorito)* con un producto *b*, esta información puede ser usada para mostrar el producto *b* a otros usuarios que encajen dentro del rango de edad *x,* usando publicidad dentro de la misma plataforma que se usó para recoger la información (Facebook, Twitter, Waze, etc). Además, productos que tengan un parecido al producto *b* pueden relacionarse —a través de publicidad— con todos aquellos usuarios que interactuaron con el mismo. La segunda finalidad usada por este tipo de empresas es la utilización de las conclusiones sacadas para mejorar el mismo producto que fue usado para obtener la información. Por ejemplo —como lo explica el artículo de *The Economist*— la información que es obtenida por Tesla a través de sus automóviles con conductores automático es usada para mejorar el servicio que prestan los mismos[4].

Estas plataformas han sido denominadas por la doctrina económica como two-sided markets. Armstrong menciona estos mercados diciendo*:* "*Many markets involve two groups of agents who interact via* "*platforms,* "*where one group's benefit from joining a platform depends on the size of the other group that joins the platform*"[5]. Ahora bien, lo particular de estos two-sided markets es que generan una externalidad positiva, en la medida en que un mayor número de gente entre al intercambio. Para nuestro caso en concreto, Facebook genera un servicio de plataforma para comunicar gente pero para la utilización de esta plataforma los usuarios de la misma dan diferente tipo de información. Por ende, se genera una externalidad, debido que entre más usuarios entren a la pla-

3 Ley Estatutaria 1581 de 2012. Art 3. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO. N 48587.

4 The world's most valuable resource is no longer oil, but data. https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource. (Mayo 6 del 2017).

5 Mark Armstrong. Competition in two sided markets. RAND Journal of Economics. Enero 2010. Página 668.

taforma, mayores incentivos se generan para que otra gente la use, generando a su vez una red de información digital más grande para Facebook[6].

Por otra parte, no solo debe verse este fenómeno desde el punto de vista cualitativo acerca de cómo es usada la información, sino desde un punto de vista cuantitativo acerca de cuánta información hay. Resulta bastante obvio que en el vivir contemporáneo Facebook se ha convertido en una necesidad para gran parte de la población. Solo para ilustrarnos cuantitativamente al respecto, resulta pertinente decir que según el portal Statista, para el año 2017, Facebook Inc. tuvo un ingreso por usuario de 20.21 dólares (U.S. Dollars)[7]. Para completar lo anterior, se debe añadir que para finales de 2017 se estimaba que existían 2,129,000,000 usuarios de Facebook activos a nivel global[8]. No hace falta ser un matemático para darse cuenta de la importancia financiera mundial con que cuenta la empresa mencionada. De ahí, que la revista *Forbes* —para el año 2017— la haya calificado como la cuarta compañía más valorada del mundo con un valor de 73.5 billones de dólares (U.S. Dollars)[9].

Ahora bien, todo lo antes mencionado de ninguna manera es dicho en términos peyorativos. Indudablemente, la información de datos puede traer muchos beneficios económicos y políticos para cualquier sociedad. No obstante, al igual que Standard Oil Company a comienzos del siglo XX y cualquier otra actividad económica, deben existir límites teniendo en consideración el bien común y los derechos fundamentales de las personas.

Todo esto ha generado —poco a poco— un esfuerzo por parte de las autoridades e instituciones de diferentes países por dar algún tipo de control al tema. Como se mostrará posteriormente, las autoridades europeas han sido las más eficientes a la hora de regular y sancionar actividades que sobrepasan los límites al uso de los datos personales recolectados en múltiples plataformas. Lastimosamente, en Colombia no ha sido tan eficiente este proceso, sin negar que de

---

6 Para mayor información acerca de los mencionados *Two-sided markets* ver:
• Marc Rysman. The Economics of Two-Sided Markets. Journal of Economic Perspectives. Summer 2009. Página 125.
• Jean-Charles Rochet & Jean Tirole. Platform Competition in Two-Sided Markets. Journal of the European Economic Association. June 2003. Página 990.

7 Facebook's annualized revenue per user from 2012 to 2017 (in U.S. dollars). https://www.statista.com/statistics/234056/facebooks-average-advertising-revenue-per-user/. (Febrero de 2018).

8 Number of monthly active Facebook users worldwide as of 4th quarter 2017 (in millions). https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/. (Enero de 2018).

9 The World's Most Valuable Brands. https://www.forbes.com/powerful-brands/list/#tab:rank. (Consultado el 17 de marzo de 2018).

poco a más se han venido haciendo avances significativos. Por ende, el presente artículo busca aportar un poco a este proceso de mejora en torno a las instituciones, autoridades, regulaciones y reglamentaciones referentes a la protección de datos personales en plataformas digitales de comunicación.

2. BREVE HISTORIA DEL CONTEXTO COLOMBIANO

Para poder llegar a entender la importancia del presente escrito es necesario primero revisar brevemente la historia de Colombia con respecto a la normativa de la protección de los datos personales. La Constitución Política de 1991 introdujo el derecho fundamental del hábeas data en su artículo 15[10]; ahora bien, no fue sino hasta la Ley Estatutaria 1266 de 2008 cuando se empezó a regular este derecho. Esta última, regula los datos personales pero solo dentro de la esfera financiera, al respecto dicha ley menciona: "*Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones*"[11]. En adicción, se puede decir que esta Ley fue un paso importante para la protección de datos en el ordenamiento jurídico colombiano, pero como alude el profesor Nelson Angarita Remolina, la misma fue precipitada[12]. El resultado del vacío dejado por esta Ley fue la expedición de la Ley Estatutaria 1581 de 2012 (Ley 1581 de 2012). Esta última y su Decreto Reglamentario 1377 de 2013 (Decreto 1377 de 2013), completaron la normativa referente a la protección de los datos personales y en consecuencia serán el cuerpo normativo usado en el presente escrito.

El 24 de noviembre del 2014, la Superintendencia de Industria y Comercio (SIC) emitió un concepto frente al tratamiento de datos personales en las redes sociales. El artículo 2 de la Ley 1581 de 2012 establece que: "*La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano*

10 Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Constitución Política de Colombia (Const). Art 15. Julio 7 de 1991 (Colombia).

11 Ley Estatutaria 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales. Diciembre 31 de 2008. DO. N 47.219.

12 Nelson Remolina-Angarita. ¿Tiene Colombia un Nivel Adecuado de Protección de Datos Personales a la luz del Estándar Europeo? Revista Colombiana de Derecho Internacional. Enero-junio de 2010. Página 509.

o cuando al responsable del tratamiento o encargado del tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana…"[13]. De acorde a lo dicho, la SIC interpretó que:

> En consecuencia, el tratamiento de los datos personales registrados en las redes sociales no encajan dentro del ámbito de competencia de la Ley 1581 de 2012, pues la recolección, el uso, la circulación, el almacenamiento o supresión de los datos personales no se realiza dentro del territorio colombiano, puesto que las redes sociales no tienen domicilio en Colombia[14].

Nelson Angarita —quien sin lugar a dudas es quien mayores aportes ha realizado a este tema en Colombia— criticó fuertemente este concepto. Su crítica puede resumirse en tres puntos concretos. Primero, la SIC omitió en su interpretación referirse a qué entiende por tratamiento de datos; esto resulta de suma importancia debido que muchos de los componentes del mismo, como la recolección, pueden ser realizados en Colombia sin necesidad de tener una sociedad domiciliada en territorio colombiano. Segundo, el artículo segundo de la referida norma nunca habla del requisito indispensable de contar con domicilio en Colombia para que le sean aplicables tales normativas. Por último, el profesor Angarita demuestra que sí existe una sociedad en las cámaras de comercio colombianas llamada FACEBOOK COLOMBIA S.A.S., por lo cual resulta ilógica la respuesta dada por la SIC[15].

Este concepto desaceleró los primeros pasos que se habían generado para la protección de datos personales en plataformas digitales en Colombia. Por suerte, el 3 de marzo del 2016, la SIC emitió un nuevo concepto enmendando su error y cambiando de forma drástica su interpretación relativa al artículo 2º de la Ley 1581 de 2012[16]. El concepto incluye varias afirmaciones bastante interesantes de mencionar. Primero, menciona como la Ley 1581 de 2012 solo hace referencia al derecho de hábeas data y no al derecho de intimidad y buen nombre. Estos derechos son independientes entre sí, en consecuencia la SIC no tiene competencia en temas referentes al buen nombre en redes sociales.

---

13 Ley Estatutaria 1581 de 2012. Art 2. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO. N 48587.

14 Concepto 2014 (Superintendencia de Industria y Comercio). Noviembre 24 de 2014. RAD: 14-218349-00003.

15 Zuckerberg, redes sociales digitales y el concepto de la Superintendencia de Industria y Comercio sobre el ámbito de aplicación de la ley colombiana de protección de datos. https://habeasdatacolombia.uniandes.edu.co/?p=1718. (Enero 13 de 2015).

16 Concepto 2016 (Superintendencia de Industria y Comercio). Marzo 3 de 2016. RAD: 14-218349-4-0.

Lo anterior es de suma importancia porque era una pregunta bastante gris, no respondida hasta el momento. Segundo, el concepto de la SIC empezó a usar normativas europeas referente al tema, lo cual muestra una profunda modernización dentro de la entidad. Lo antepuesto se puede reflejar cuando se define dentro del concepto qué es el servicio de red social y sus características[17]. La SIC menciona que estas definiciones se extrajeron del trabajo realizado por el Grupo de Trabajo del artículo 29, en el Informe de Trabajo No. 163. Lo último es explicado diciendo:

> "Este Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente sobre la protección de datos y la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE"[18].

Por último, y también utilizando normativa europea —artículo 29 de la directiva 95/46/CE—, la SIC expresa su cambio en materia de competencia diciendo:

> En otras palabras, la SIC se encuentra completamente facultada para garantizar el tratamiento de datos personales de los colombianos que, a través de las redes sociales en internet compartan información personal; todo en observancia de los principios, derechos, garantías y procedimientos establecidos por la Ley 1581 de 2012[19].

Esto, basado en el argumento propuesto en la directiva 95/46/ CE, el cual afirma: "…*los PC, los terminales y los servidores, que se pueden utilizar para casi todos los tipos de operaciones de tratamiento de datos, son ejemplo de medio*"[20]. En otras palabras —como se explicará con mucho más detalle en los siguientes folios—, el tratamiento de datos se realiza a través de cookies que se encuentran físicamente dentro del disco duro del PC. Por ende, sí es posible aplicar el clásico principio de territorialidad de la ley.

---

17 Para efectos de mayor entendimiento del artículo, la SIC define servicio de red social como: plataformas de comunicación en línea que permiten a los individuos crear redes sociales que comparten intereses comunes y sus características son: los usuarios deben proporcionar datos personales para generar su descripción o perfil. Proporcionan también herramientas que permiten a los usuarios poner su propio contenido en línea (contenido generado por el usuario como fotografías, crónicas o comentarios, música, vídeos o enlaces hacia otros sitios). funcionan gracias a la utilización de herramientas que proporcionan una lista de contactos para cada usuario, con las que el usuario puede interactuar. Concepto 2016 (Superintendencia de Industria y Comercio). Marzo 3 de 2016.

18 Concepto 2016 (Superintendencia de Industria y Comercio). Marzo 3 de 2016.

19 Concepto 2016 (Superintendencia de Industria y Comercio). Marzo 3 de 2016.

20 Autoridad colombiana de protección de datos concluye que sí es competente para investigar a Facebook. https://habeasdatacolombia.uniandes.edu.co/?p=2190. (Marzo 16 de 2016).

Habiendo visto todo lo anterior, se puede hacer una breve pero importante conclusión: solo hasta el año 2016 en Colombia —con el concepto se la SIC— se aceptó la existencia de una autoridad con potestades sancionatorias en materia de datos personales en servicios de redes sociales. Ahora bien, tal como menciona este mismo concepto, no existen procesos o investigaciones en curso, por lo cual —si se quiere llegar a hacer uno— es de notoria importancia que se revisen y analicen los procesos sancionatorios llevados a cabo en otros países. Es ahí, donde el presente artículo toma relevancia, al examinar cuidadosamente la resolución R/01870/2017 y poder llegar a conclusiones que generen un aporte a lo doctrina y práctica colombiana.

3. BREVE HISTORIA Y CONTEXTO EUROPEO

Teniendo en consideración que la finalidad máxima de este escrito es poder llegar a mejorar nuestro ordenamiento jurídico sobre protección de datos personales con base en una resolución europea, es necesario explicar brevemente el contexto e historia europea sobre el tema. Todo esto con la perspectiva de hacer interpretaciones correctas.

La génesis de la protección de datos personales en Europa se dio a través de las resoluciones 509 de 1968, de la Asamblea del Consejo de Europa que versa sobre los derechos humanos y los nuevos logros científicos y técnicos[21]. Lo anterior generó el nacimiento de una inquietud acerca de la relación entre la intimidad y los datos personales. Como resultado de esta inquietud, en 1973, se expidió la Resolución 22 del Comité de Ministros de Europa, la cual recomienda a los Gobiernos de los Estados miembros a tomar medidas relativas tanto en el sector privado como en el público. Estas medidas son resumidas por el profesor Miguel Ángel Davara: *"Las personas que deban operar sobre las bases de datos tienen que estar bajo normas severas de conducta para el mantenimiento del secreto y poder prevenir el mal uso de los datos*"[22]. Tan solo un año después este mismo comité expide la Resolución 29, haciendo parecidas recomendaciones sobre los bancos electrónicos del sector público. Lo expuesto resulta importante debido que —por más de haber sido expedidas estas normativas en los años 70— siguen estando vigente y son la base de las normas siguientes. En palabras del profesor Davara: "*Es conveniente señalar que los principios y*

21 Lo Dicho se genera debido a una comisión Consultiva establecida por el Consejo de Europa en 1967, con el fin de estudiar las tecnologías y su respectiva repercusión en los derechos de las personas.

22 Miguel Ángel Davara. La Protección de Datos en Europa. Pág 31. Ed., Grupo Asnef Equifax. (1998).

derechos que se recogían en aquellos escritos siguen teniendo vigencia y plena actualidad hoy en día, aunque, como es lógico, adecuados y adaptados a la evolución social y tecnológica"[23].

Por otra parte, las recomendaciones realizadas por la OCDE el 23 de septiembre de 1980, también pueden ser señaladas como raíz normativa acerca de la protección de datos personales. Reproduciendo lo citado por el profesor Angarita en su libro *Tratamiento de datos personales,* en relación con lo dicho por la OCDE:

> Los países miembros deberían establecer procedimientos o instituciones jurídicas, administrativas u otras para la protección de la intimidad y las libertades individuales respecto de los datos personales. Los países miembro deberían en particular: a) adoptar legislación nacional adecuada; b) fomentar y apoyar la autorregulación, ya sea en forma de códigos de conducta o de otro modo; c) prever las sanciones y recursos suficientes en caso de incumplimiento de las medidas con las cuales se implanten los principios expuestos en las partes II y III y e) asegurar que no haya discriminación injusta contra los sujetos de los datos[24].

Es debido a estos principios y recomendaciones que el Consejo de Europa expide el Convenio 108 para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal en 1981. Concerniente a este Convenio es propicio citar dos artículos. El artículo primero menciona el objeto del mismo: "*Garantizar en el territorio de cada parte, a cualquier persona física, el derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal*"[25]. Con lo anterior, se puede ver la concreción de una normativa dedicada a la relación entre los datos personales y el derecho a la intimidad. Segundo, es menester decir que el artículo 4.1 indica: "*Cada parte adoptará en su derecho interno las medidas necesarias para dar cumplimiento a los principios fundamentales de protección de datos enunciados en el presente capítulo*"[26]. El anterior artículo presenta una premisa de tremenda importancia para tener siempre presente, el Convenio 108 solo delimi-

23 Miguel Ángel Davara. La Protección de Datos en Europa. Pág 30. Ed., Grupo Asnef Equifax. (1998).

24 Nelson Remolina Angarita. Tratamiento de datos personales. Pág 17. Ed., Legis Editores S.A. (2013).

25 Convenio (108) para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal. Artículo 1. Enero 28, 1981.

26 Convenio (108) para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal. Artículo 4.1. Enero 28, 1981.

ta los principios normativos acerca del tema, pero corresponde a cada Estado miembro llenar este marco normativo. Por lo anterior, debe quedar claro que cada país miembro europeo tiene su normativa propia acerca de la protección de datos personales y pueden llegar a diferir en determinados aspectos, eso sí, teniendo todos los mismos principios.

Ya para finalizar, cabe mencionar la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995 (Directiva 95/46/CE), relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. La anterior normativa fue clave a la hora de generar definiciones claras acerca de términos tecnológicos, con lo cual se logró evitar debates jurídicos sobre los mismos.

Como se mencionó anteriormente, cada Estado miembro de la Unión Europea tiene el deber de expedir su propia normativa para hacer cumplir lo dicho en el Convenio 108. Teniendo en consideración que el ejercicio comparativo a realizar es con base en una resolución española, se tiene que decir que la ley española de protección de datos es la Ley Orgánica 5 de 1992, del 29 de octubre (Ley 5 de 1992). Para finalizar, uno de los aspectos más trascendentes de esta Ley 5 de 1992 es la creación —por virtud del artículo 34— de la Agencia de Protección de Datos, la cual tiene personalidad jurídica propia y plena independencia de las administraciones públicas. En virtud de esta agencia se realizan los procesos sancionatorios y la misma procura velar por el cumplimiento tanto de la Ley Orgánica 5 de 1992 española como todas las normativas europeas relativas a la protección de datos personales[27]. Por último, esta Ley fue derogada por la Ley Orgánica 15 de 1999 (Ley 15 de 1999), la cual actualizó la normativa relativa a la protección de datos personales pero mantuvo la esencia de la primera norma mencionada.

4. CASO EN CONCRETO

4.1. RESPONSABILIDAD

Para el análisis del presente caso se llevará el orden implementado en los fundamentos de derecho expuestos en la Resolución R/01870/2017 de la Agencia Española de Protección de Datos Personales. A medida que se vayan mostrando los determinados fundamentos se hará la correspondiente comparación con la legislación colombiana.

27 Ley Orgánica 5 de 1992. Art 36. De regulación del tratamiento automatizado de los datos de carácter personal. Octubre 29 de 1992. BOE. Octubre 31 de 1992.

El primer punto a tratar, es en cabeza de quién se encuentra la responsabilidad en el tratamiento de datos personales de los usuarios de Facebook. Al respecto caben precisar los siguientes hechos:

- El 7 de marzo de 2017 la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a Facebook Inc.[28].

- Facebook Inc. es la sociedad matriz de Facebook, la cual se sita en Delaware y tiene domicilio en Menlo Park, California[29].

- El 31 de marzo de 2017 Facebook Inc. hizo llegar un escrito a la Agencia Española de Protección de Datos aduciendo que ellos no tenían ningún tipo de responsabilidad en el proceso llevado a cabo debido que la responsabilidad estaba en cabeza de Facebook Ireland[30].

Lo anterior, se basa en la página de condiciones del servicio español de Facebook, las cuales mencionan según lo dicho por la Agencia Española de Protección de Datos Personales:

> Si resides o tienes tu sede de actividad comercial principal en EE. UU. o Canadá, esta Declaración constituye el acuerdo entre Facebook, Inc. y tú. De lo contrario, esta Declaración constituye el acuerdo entre Facebook Ireland Limited y tú. Las menciones a "nosotros", "nos" y "nuestro" se refieren a Facebook, Inc. o Facebook Ireland Limited, según corresponda[31].

Pasando a responder la pregunta —quién tiene la responsabilidad— la Agencia Española de Protección de Datos se basó en un precedente para llegar a la respuesta. Dicho caso es Google Inc. vs Costeja. Harvard Law review trae un conciso y claro resumen del caso:

---

28 Resolución: R/01870/2017. Pg 1. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

29 Resolución: R/01870/2017. Pg 3. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

30 Resolución: R/01870/2017. Pg 4. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

31 Resolución: R/01870/2017. Pg 3. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.
Cabe decir que desde un servidor colombiano se puede encontrar estipulado exactamente lo mismo. https://www.facebook.com/legal/terms (Enero 20 de 2015).

> On March 5, 2010, Mario Costeja González, a Spanish citizen, lodged a complaint with the Spanish data protection agency, AEPD, against a Spanish newspaper, Google Spain SL ("Google Spain"), and Google Inc. An Internet user typing Costeja González's name into Google's search engine would receive links to two newspaper pages announcing a foreclosure auction on Costeja González's home. In his complaint, Costeja González requested first that the newspaper be required to remove his name, and second that Google Spain "remove or conceal" his personal data so that they no longer appeared in the search results. Costeja González argued that because the attachment proceedings had been "fully resolved[,] … reference to them was now entirely irrelevant," and he had the right to have the data removed. The AEPD denied Costeja González's complaint against the newspaper, but granted it against Google[32].

Al final, Google Inc. termina perdiendo el caso y es obligado a remover la información del señor Costeja pero independientemente de eso, lo interesante fue la defensa propuesta por Google. Al igual que Facebook, Google afirma que no es responsable sino otra sociedad de la misma llamada Google Search.

En dicha resolución se expone un argumento bastante importante para traer a colación. La directiva 95/46/CE, estipula tres componentes para determinar el responsable del tratamiento de la protección de datos: el aspecto personal, la posibilidad de control plural y los elementos esenciales para distinguir al responsable de otros agentes a través de la determinación de fines y medios en el tratamiento. Cuando se hace referencia a la determinación del fin debe entenderse que esta solo podrá ser realizada por el encargado. En oposición cuando se hace referencia a la determinación de los medios debe entenderse que esta podrá ser delegada por parte del encargado[33].

Es por todo lo mostrado, que la Agencia Española de Protección de Datos, desestimó las alegaciones hechas por Facebook Inc. Usando los criterios de interpretación dados, claramente se puede concluir que Facebook Inc. sí es responsable del tratamiento debido que son ellos quienes evidentemente determinan los fines y las cuestiones de fondo al ser la sociedad matriz.

---

32 Internet Law- Protection of Personal Data- Court of Justice of the European Union creates presumption that Google must remove links to personal Data upon request.- Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos. Harvard Law Review. Mayo 13 de 2014. Página 735.

33 Resolución: R/01870/2017. Pg 69. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

Teniendo en consideración que —desde un servidor colombiano— Facebook también menciona en sus políticas que las relaciones contractuales existentes son con Facebook Ireland y en consecuencia Facebook Inc. no tiene ningún tipo de responsabilidad, al analizar cómo se resolvería el caso bajo la legislación colombiana es necesario remitirse a dos conceptos que nos trae la Ley 1581 de 2012. El primero de ellos es el de encargado del tratamiento, el cual es definida 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*"[34]. El segundo, es el de responsable del tratamiento, el cual es definido 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 tratamiento de datos*"[35]. Por último cabe añadir que ambos se les exigen determinados deberes contemplados en los artículos 17 y 18 de la descrita ley.

Como se puede evidenciar la diferencia que radica entre el responsable del tratamiento y el encargado se encuentra en el verbo decidir y realizar. Siendo el primero relacionado con el responsable y el segundo con el encargado. En adición, se puede deducir de los artículos 17 y 18 de la Ley 1581 de 2012, que la diferencia principal entre el responsable y encargado radica en el deber de información que tiene el responsable de decir al titular de los datos personales, la finalidad de la recolección y los derechos que le asisten por haber aceptado dicha recolección[36]. Póstumo, cabe decir que el artículo 23 menciona que las sanciones por incumplimiento pueden ser tanto para el responsable como el encargado[37], por lo cual no cabe duda que Facebook Ireland, sí tendría responsabilidad en el caso por ser sujeto del vínculo contractual existente. Ahora bien, por más de saber que tiene responsabilidad, cabría hacer la pregunta si la tiene en calidad de encargado o responsable y a su vez si Facebook Inc. también tendría responsabilidad, ya sea por ser encargado o responsable.

A la hora de determinar si Facebook Inc. tiene responsabilidad en el caso —bajo la ley colombiana— nos encontramos que habría que determinar si es el responsable o el encargado, ateniendo que el criterio diferenciador está en la

34 Ley Estatutaria 1581 de 2012. Art 3. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO. N 48587.

35 Ley Estatutaria 1581 de 2012. Art 3. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO. N 48587.

36 Ley Estatutaria 1581 de 2012. Art 17 y 18. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO. N 48587.

37 Ley Estatutaria 1581 de 2012. Art 23. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO. N 48587.

acción de realizar y decidir. Ahora bien, teniendo en consideración que la sociedad matriz es quién tiene un control jurídico sobre sus subsidiarias, se podría concluir que Facebook Inc. es quien decide sobre las actividades a realizar de Facebook Ireland. Por ende, el primero sería el responsable y el segundo el encargado. Como se mostró anteriormente, por más de que los términos y condiciones estipulen que si resides o tienes actividad comercial por fuera de EE.UU o Canadá, el vínculo contractual será con Facebook Ireland, al Facebook Inc. tener capacidad de control y decisión sobre las decisiones de Facebook Ireland; este se convierte en el responsable de los mismos y también —junto con el encargado, Facebook Ireland— podrá ser sancionado por la legislación colombiana de protección de datos[38]. Todo esto, usando los términos realizar y decidir en abstracto ya que no han sido explicados por la SIC a través de resoluciones o conceptos. Lo anterior, se contrapone a criterios, definiciones y jurisprudencia mucho más concretas y claras determinadas por la normativa europea. Será la SIC quien a través de sus futuras resoluciones y conceptos dé interpretaciones con muchos más detalles, que puedan ayudar a definir este tema que puede generar muchas controversias.

4.2. CONSENTIMIENTO

Corresponde ahora analizar el tema concerniente al consentimiento por parte del titular de los datos personales en el tratamiento de los mismos. Es necesario decir que tanto las leyes españolas como las colombianas contemplan este requisito en sus normativas. Al respecto la Ley 15 de 1999 expresa en su título II, artículo 4.1 y 4.2:

> **Artículo 4.** *Calidad de los datos.*
>
> 1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
>
> 2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos[39].

38 Ley Estatutaria 1581 de 2012. Art 22. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO. N 48587.

39 España. Ley Orgánica 15 de 1999. Art 4.1 y 4.2. De protección de Datos de Carácter Personal. Diciembre 13 de 1999. BOE. No. 298. Diciembre 14 de 1999.

Cabe decir que la jurisprudencia española ha llamado el numeral primero de este artículo como el principio de proporcionalidad, en el entendido de que "*solo pueden ser sometidos a tratamiento aquellos datos que sean estrictamente necesarios para la finalidad perseguida*"[40]. Por otro lado, la normativa colombiana —Ley 1581 de 2012— estipula en su artículo 4, literal b y c:

> b) **Principio de finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;
>
> c) **Principio de libertad:** El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento[41].

Para empezar, cabría mencionar que la normativa colombiana no crea un nexo de proporcionalidad entre la finalidad y el consentimiento. En otras palabras, no dan un límite al tratamiento de los mismos, siempre y cuando el fin sea legítimo y haya habido un consentimiento previo, expreso e informado por parte del titular. No obstante, ambas normativas no dejan duda alguna acerca de la autorización informada que debe haber previa al tratamiento de los datos.

Habiendo visto lo anterior, cabe analizar lo dicho por la Agencia Española de Protección de Datos: primero, al momento de hacer el registro inicial en la página de Facebook y leer sus Políticas de Privacidad, se usan expresiones genéricas y ambiguas, además de tener que usar varios enlaces para poder leer la totalidad del mismo. Segundo, se afirma que una persona con calidad media en conocimiento informático no logra entender en su totalidad el tratamiento al cual van a ser acogidos sus datos. Por último, mencionan que sus organismos de investigación, han demostrado que es posible aceptar las Políticas de Privacidad de la página sin que verdaderamente se obligue al usuario a leerlas[42].

Es necesario hacer un alto en el camino para tratar de explicar varios puntos con mayor profundidad. Es inevitable hacer anotaciones respecto a cómo son

---

40 Resolución: R/01870/2017. Pg 82. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

41 Ley Estatutaria 1581 de 2012. Art 4, literal b y c. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO. N 48587.

42 Resolución: R/01870/2017. Pg 82 y 83. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

las políticas de Facebook en Colombia, cómo funciona la recolección de datos y por último qué datos se recogen en esta plataforma digital.

Para la fecha del primero de Abril del año 2018, entrando desde un servidor colombiano se puede corroborar que es necesario acudir a varios enlaces distintos para lograr leer la totalidad de políticas que maneja Facebook. Estas se dividen en políticas de privacidad, cookies y términos de condiciones. Es evidente que por cuestiones de espacio es imposible poder trasmitir todo lo que dicen cada una de estas y solo nos daremos la misión de dar breves comentarios al respecto. No obstante, se recomienda leer la totalidad de las mismas para comprender de mejor manera el tema[43].

Acerca de las políticas de datos, cabe hacer dos apreciaciones importantes, la primera de ellas es que al igual que en España, se dice que el responsable de los datos personales tratados en Colombia, no es Facebook Inc., sino Facebook Ireland Ltd. Al detalle, la página menciona que si vives en un país diferente a Estados Unidos o Canadá:

> *"La entidad de control de datos responsable de tu información es Facebook Ireland Ltd., con la que te puedes poner en contacto en internet* o por correo postal en la dirección:
>
> *Facebook Ireland Ltd. 4 Grand Canal Square Grand Canal Harbour Dublín 2, Irlanda*"[44].

También, se hace la acotación que la última modificación realizada, fue el 29 de septiembre de 2016. Como se podrán dar cuenta, esta fecha es anterior a la sanción dada por la Agencia Española de Protección de Datos Personales, lo cual nos lleva a concluir, que por lo menos entrando desde un servidor colombiano, Facebook no trata de corregir los errores que han sido encontrados por parte de otros ordenamientos jurídicos, aun cuando han sido sancionados monetariamente por ello.

Las políticas de términos y condiciones, nos traen unas conclusiones bastante interesantes. Estas políticas comienzan diciendo lo siguiente: "*This agree-*

---

43 Declaración de derechos y responsabilidades. https://www.facebook.com/legal/terms (Enero 20 de 2015).
Políticas de datos. https://www.facebook.com/about/privacy (Septiembre 29 de 2016).
Cookies y otras tecnologías de almacenamiento. https://www.facebook.com/policies/cookies (Marzo 20 de 2017).

44 Políticas de datos. https://www.facebook.com/about/privacy (Septiembre 29 de 2016).

ment was written in English (US). To the extent any translated version of this agreement conflicts with the English version, the English version controls"[45]. Es bastante curioso que los términos y condiciones no hagan diferencia entre si uno se encuentra en Estados Unidos y Canadá o en otro lugar del mundo. Lo anterior, con el propósito de hacer referencia a las leyes propias de protección de datos de cada ordenamiento jurídico. En adición, se debe comentar que —al igual que se expresó la Agencia Española de Protección de Datos— resulta difícil que una persona con un mediano conocimiento en temas de datos personales logre entender a cabalidad el funcionamiento de tratamiento y además pueda entender el texto legal en inglés. Como bien se citó anteriormente, solo es vinculante para las partes lo escrito en inglés y no lo traducido; esto, genera problemas debido que se requiere un conocimiento amplio en derecho comparado para entender la terminología usada en otros ordenamientos jurídicos, por más de conocer la terminología jurídica local.

Sabiendo de la ambigüedad usada en las políticas dadas por Facebook, cabe hacer mención a la pregunta: ¿cómo funciona la recolección de datos por parte de Facebook? El Grupo de Trabajo sobre Protección de Datos[46] comentó lo siguiente acerca de los cookies:

> The controller decides to collect personal data by means of a text file (cookie), which is placed on the hard disk of the user's personal computer, while a copy might be kept by the web site or a third party. In the case of further communication, the information stored in the cookie (and therefore in the user PC) is accessed by the web site in order to identify this PC to the controller. The controller is thus enabled to link up all information he has collected during previous sessions with information he collects during subsequent sessions. In this way, it is possible to create quite detailed user profiles[47].

De lo anterior, se pueden sacar dos conclusiones. Primero, este mecanismo mediante el cual se recolectan datos, se encuentra localizado en el disco duro de todo usuario que haya interactuado con el cookie. Segundo, las páginas web que hayan instalado estos cookies, tienen acceso a ellos para extraer la informa-

45 https://www.facebook.com/legal/terms (Enero 20 de 2015).

46 Este Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente sobre la protección de datos y la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

47 Working document 5035/01/EN (Data Protection Working Party). Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites. May 30 of 2002.

ción. Por último, cabe recordar lo dicho anteriormente: debido que estos cookies se encuentran en el disco duro del usuario, se puede alegar la competencia en procesos sancionatorios por virtud del principio de territorialidad[48]. Ahora bien, habiendo entendido qué es un cookie, resulta pertinente saber qué información es recogida por este.

Por más de ser un poco tedioso leer lo que se encuentra a continuación, se considera vital tener esta información para verdaderamente tener un conocimiento informado acerca del tipo de información que esta plataforma tiene sobre uno. A continuación, se mostrará qué información se tiene disponible sobre el titular de la información, y se pondrá en negrilla todas aquellas que el autor considere que puedan llamar particularmente la atención:

1) Acerca de mí, haciendo referencia a toda la biografía puesta en la plataforma. 2) Historial de estados de la cuenta, haciendo referencia a la desactivación y reactivación de la misma. 3) **Sesiones activas**, haciendo referencia a todas las sesiones activas almacenadas, con inclusión de la fecha, la hora, el dispositivo, la dirección IP y la información sobre el navegador y las cookies del dispositivo. 4) **Anuncios en los que has hecho clic**. 5) Dirección. 6) **Temas de los anuncios**, hace referencia a la lista de los temas por los que se te podría segmentar en función de los gustos y los intereses que has especificado y de otros datos que constan en tu biografía. 7) Nombre alternativo. 8) Aplicaciones. 9) Visibilidad de tu fecha de nacimiento. 10) **Chat**, haciendo referencia a todos los historiales de conversaciones que hayas tenido. 11) Vistas. 12) Conexiones. 13) **Tarjetas de Crédito**, si haces compras por Facebook. 14) Divisa, si haces compras por Facebook. 15) Ciudad actual. 16) Fecha de nacimiento. 17) Amigos eliminados. 18) Formación. 19) Correos electrónicos, incluso si la has eliminado. 20) Eventos. 21) **Datos de reconocimiento facial**, basado en fotos en que hayas sido etiquetado. 22) Familia. 23) Citas favoritas. 24) Seguidores. 25) Personas y páginas que sigues. 26) Solicitudes de amistad. 27) Amigos. 28) Sexo. 29) Grupos. 30) Elementos ocultados en la sección de noticias. 31) Ciudad de origen. 32) **Direcciones IP**. 33) Última ubicación. 34) Veces que has indicado que te gustan las publicaciones de otros. 35) Personas a las que han gustado tus publicaciones. 36) Veces que has hecho clic en "me gusta" en otros sitios, haciendo referencia a páginas web diferentes a Facebook. 37) Cuentas vinculadas. 38) Idioma. 39) Inicios de sesión. 40) Cierres de sesión. 41) **Mensajes**. 42) Nombre. 43) Cambios de nombre. 44) Redes. 45) **Notas**, haciendo referencia a todo lo escrito y publicado en tu cuenta. 46) Configuración de las notificaciones. 47) Páginas que administras. 48) Solicitudes de amistad pendientes. 49)

48 Ibidem, página 7-8.

Números de teléfono. 50) **Fotos.** 51) Metadatos de fotos. 52) Elementos físicos. 53) Toques. 54) Ideología política. 55) Tus publicaciones. 56) Publicaciones de otras personas, en tu biografía. 57) Publicaciones en otras personas. 58) Configuración de la privacidad. 59) Actividades recientes. 60) Fecha de registro. 61) Creencias religiosas. 62) Videos. 63) Nombre de usuario. 64) Búsquedas. 65) Contenido compartido. 66) Idiomas conocidos. 67) Actual de estado. 68) **Empleo.** 69) URL personalizada[49].

Habiendo visto qué tipo de datos recogen los cookies y cómo es el funcionamiento de los mismos, se concluye que esto se hace de forma poco transparente y con una gran difusión. En consecuencia, no debe ser posible que el consentimiento para aceptar que sean recopilados los datos sea a través de un proceso sencillo o automatizado. La aceptación debe ser inequívoca y no solo haciendo clic sin que exista un verdadero convencimiento de saber el contenido de dicha aceptación[50].

Diversas conclusiones se pueden desprender de la última parte de este escrito. Primero, el ordenamiento jurídico colombiano no incorpora el principio de proporcionalidad como sí lo hace el ordenamiento jurídico español. No obstante, es tal la ambigüedad de las políticas, términos y condiciones de Facebook Inc., que no hace falta hilar tan delgado para darse cuenta que el consentimiento por parte del usuario no es inequívoco. En otras palabras, no hace falta aplicar el principio de la proporcionalidad —ni en Colombia o España— para lograr demostrar el incumplimiento por parte de Facebook Inc., a la hora de ejercer el tratamiento de datos personales con el consentimiento, previo, expreso e informado del titular. Ahora bien, esto no significa que en un futuro —por el hecho de no incluir en la Ley 1581 de 2012, el principio de proporcionalidad— se vuelva más complicado poder resolver un caso en concreto en el cual no sea tan obvio el incumplimiento por parte del responsable.

En segunda medida, se concluye que el análisis realizado a las políticas y términos y condiciones de Facebook desde un servidor colombiano, es posterior al proceso sancionatorio efectuado por la Agencia Española de Datos, parece ser que las lecciones solo se aprendieron en territorio español. Tanto es así, que observando las políticas, términos y condiciones de Facebook Inc. —desde un

49 Resolución: R/01870/2017. Pg 19, 20, 21, 22, 23, 24 y 25. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

50 Resolución: R/01870/2017. Pg 83. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

servidor colombiano— no se hace referencia a la Ley 1581 del 2012. Irónicamente, como ya se mostró, Facebook Inc. cuenta con una sociedad en Colombia.

4.3. CANCELACIÓN DE DATOS

Por último, falta hablar de la utilización de los datos personales después de su cancelación por parte del titular. Esta puede ser una de las faltas más graves y menos conocidas por parte de los usuarios de Facebook.

La Agencia Española de Protección de Datos logró probar que posterior a la cancelación de una cuenta por parte del usuario, Facebook conserva las direcciones IP por términos de hasta 11 meses[51]. Además, si a través de cookies o direcciones IP logra identificar una nueva cuenta de la misma persona, agrupa su información anterior con la usada en la nueva cuenta. En adición, los cookies de las cuentas eliminadas siguen recolectando y tratando información del usuario hasta por 17 meses[52]. En otras palabras, los cookies —los cuales como se mencionó anteriormente se encuentran en el disco duro del computador a través del cual se ingresa a la cuenta de Facebook— no se desactivan luego de la eliminación de las cuentas y siguen recolectando los datos del usuario cuando este realiza interacciones con su dispositivo electrónico. Por más de que ya no se puede recolectar información con base a su interacción con Facebook directamente, sí se recolecta información bastante útil cómo la localización, tiempo de uso del dispositivo y programas usados[53].

Lo anterior, contraviene claramente el artículo 4.5 de la Ley 15 de 1999 que establece[54]:

> Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

---

51 Resolución: R/01870/2017. Pg 88. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

52 Resolución: R/01870/2017. Pg 67, 68 y 88. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

53 Resolución: R/01870/2017. Pg 88. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

54 Además del artículo mencionado también se protege la cancelación de datos en los artículos 16.2 y 16.5 de la misma ley.

> No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados[55].

En contraposición, la Ley de nuestro ordenamiento jurídico colombiano no estipuló de manera clara esta disposición. La Ley 1581 de 2012, menciona que a través de un reclamo por parte del titular se podrá corregir, actualizar o suprimir la información cuando se genere un incumplimiento a los deberes establecidos por esta Ley.

> **Artículo 15.** ***Reclamos.*** El Titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en esta ley[56].

Fue gracias al Decreto Reglamentario 1377 de 2013 que el poder ejecutivo introdujo esta política de eliminación, ante el vacío jurídico que había sido creado por la Ley Estatutaria. Es así como el artículo 11 del susodicho decreto expresa:

> **Artículo 11.** ***Limitaciones temporales al Tratamiento de los datos personales***. Los Responsables y Encargados del Tratamiento solo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la o las finalidades del tratamiento y sin perjuicio de normas legales que dispongan lo contrario, el Responsable y el Encargado deberán proceder a la supresión de los datos personales en su posesión. No obstante lo anterior, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual[57].

Es así, como se corrigió esta impertinencia, por lo cual se puede hacer la conclusión que el Decreto 1377 de 2013 no solo debe ser visto como una nor-

---

55 España. Ley Orgánica 15 de 1999. Art 4.5. De protección de Datos de Carácter Personal. Diciembre 13 de 1999. BOE. No. 298. Diciembre 14 de 1999.

56 Ley Estatutaria 1581 de 2012. Art 15, literal b y c. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO. N 48587.

57 Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Junio 27 de 2013.

mativa de ejecución de la Ley 1581 de 2012 sino también como una norma con importantes cuestiones sustanciales a analizar.

6. CONCLUSIONES.

Habiendo terminado el análisis del caso propuesto, se pueden resaltar las siguientes conclusiones al respecto:

- Facebook Inc. sí es responsable por el tratamiento de los datos personales recolectados desde servidores y ordenadores colombianos. Independientemente que las políticas de Facebook, estipulan que el vínculo contractual existente es con Facebook Ireland, la responsabilidad de este último no es única y se comparte con Facebook Inc. debido que Facebook Inc. es quien decide la finalidad del tratamiento de los datos personales y —además— ejerce un poder de control jurídico sobre Facebook Ireland.
- Facebook no hace referencia a la normativa colombiana en sus políticas.
- Por más de haber sido sancionado por otros ordenamientos jurídicos, Facebook no realiza ningún cambio en sus políticas de datos, cookies y condiciones.
- Para poder ser resueltos los problemas referentes a la protección de datos personales, no solo debe ser vista la Ley 1581 de 2012 sino también el Decreto 1377 de 2013, debido al importante contenido en algunas materias que trae el mismo.

La conclusión más importante a realizar es repetir que de ningún modo el tratamiento de los datos personales es una cuestión negativa. Esto puede tener consecuencias bastante positivas desde un punto de vista económico y político. Ahora bien, lo anterior no significa que se puede llevar a cabo esta actividad de forma anárquica. La misma requiere de límites, responsabilidad y mecanismos de control. Lastimosamente en Colombia por más de existir límites planteados en la ley, los mismos no se hacen efectivos por la falta de efectividad y control de determinadas instituciones.

BIBLIOGRAFÍA

1. Autoridad colombiana de protección de datos concluye que sí es competente para investigar a Facebook. https://habeasdatacolombia.uniandes.edu.co/?p=2190. (Marzo 16 de 2016).
2. Cookies y otras tecnologías de almacenamiento. https://www.facebook.com/policies/cookies. (Marzo 20 de 2017).

3. Concepto 2014 (Superintendencia de Industria y Comercio). Noviembre 24 de 2014. RAD: 14-218349- -00003.

4. Concepto 2016 (Superintendencia de Industria y Comercio). Marzo 3 de 2016. RAD: 14-218349 -4-0.

5. Constitución Política de Colombia (Const). Julio de 1991 (Colombia).

6. Convenio (108) para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal. Enero 28, 1981.

7. Declaración de derechos y responsabilidades. https://www.facebook.com/legal/terms. (Enero 30 de 2015).

8. Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Junio 27 de 2013.

9. Facebook's annualized revenue per user from 2012 to 2017 (in U.S. dollars). https://www.statista.com/statistics/234056/facebooks-average-advertising-revenue-per-user/. (Febrero de 2018).

10. Internet Law- Protection of Personal Data- Court of Justice of the European Union creates presumption that Google must remove links to personal Data upon request.- Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos. Harvard Law Review. Mayo 13 de 2014. Página 735.

11. Jean-Charles Rochet & Jean Tirole. Platform Competition in Two-Sided Markets. Journal of the European Economic Association. June 2003. Página 990.

12. Ley Estatutaria 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales. Diciembre 31 de 2008. DO. N 47.219.

13. Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012. DO. N 48587.

14. Ley Orgánica 5 de 1992. De regulación del tratamiento automatizado de los datos de carácter personal. Octubre 29 de 1992. BOE. Octubre 31 de 1992.

15. Mark Armstrong. Competition in two sided markets. RAND Journal of Economics. Enero 2010. Página 668.

16. Marc Rysman. The Economics of Two-Sided Markets. Journal of Economic Perspectives. Summer 2009. Página 125.

17. Miguel Ángel Davara. La Protección de Datos en Europa. Ed., Grupo Asnef Equifax. (1998).

18. Nelson Remolina-Angarita. ¿Tiene Colombia un Nivel Adecuado de Protección de Datos Personales a la luz del Estándar Europeo? Revista Colombiana de Derecho Internacional. Enero-junio de 2010. Página 489.

19. Nelson Remolina Angarita. Tratamiento de datos personales. Ed., Legis Editores S.A. (2013).

20. Number of monthly active Facebook users worldwide as of 4th quarter 2017 (in millions). https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/. (Enero de 2018).

21. Política de datos. https://www.facebook.com/about/privacy. (Septiembre 29 de 2016).

22. Resolución: R/01870/2017. (Agencia Española de Protección de datos). En el procedimiento sancionador PS/00082/2017, instruido de oficio por la Agencia Española de Protección de Datos a la entidad FACEBOOK, INC. Agosto 21 de 2017.

23. The World's Most Valuable Brands. https://www.forbes.com/powerful-brands/list/#tab:rank. (Consultado el 17 de marzo de 2018).

24. The World's Most Valuable Resource Is No Longer Oil, But Data. https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource. (Mayo 6 del 2017).

25. Wall Street starts to trim Facebook targets as shares fall. https://www.reuters.com/article/us-facebook-stocks/wall-street-starts-to-trim-facebook-targets-as-shares-fall-idUSKBN1GX1MI. (Marzo 21 del 2018).

26. Working Party 5035/01/EN (Data Protection Working Party). Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites. Mayo 30 de 2002.

27. Zuckerberg, redes sociales digitales y el concepto de la Superintendencia de Industria y Comercio sobre el ámbito de aplicación de la ley colombiana de protección de datos. https://habeasdatacolombia.uniandes.edu.co/?p=1718. (Enero 13 de 2015).