REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RESOLUCIÓN NÚMERO 1321 DE 2019

(24 ENE. 2019)

"Por la cual se imparten órdenes dentro de una actuación administrativa"

VERSIÓN PÚBLICA

Radicación 18-233402

EL DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES

En ejercicio de sus facultades legales, en especial las conferidas por los artículos 19 y 21 de la Ley 1581 de 2012 y el artículo 17 del Decreto 4886 de 2011, y

CONSIDERANDO

PRIMERO: Que la protección de datos personales es un derecho constitucional y fundamental en la República de Colombia. El artículo 15 de la Constitución Política, exige que en la recolección, tratamiento y circulación de los datos personales se respeten la libertad y demás garantías consagradas en la Constitución.

El término tratamiento se refiere a "*cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.*" [1]. Para garantizar un debido tratamiento de los datos personales es imperioso implementar, entre otras, todas las medidas de seguridad necesarias, apropiadas, útiles y eficaces para impedir que la información de las personas sea objeto de acceso, consultas, circulación, adulteración, pérdida o uso no autorizado o fraudulento[2].

Las medidas de seguridad que no reúnan las características mencionadas o que incumplan los objetivos señalados ponen en riesgo algunos derechos humanos y convierten el tratamiento de datos personales en una actividad indebida e inconsistente con los mandatos constitucionales y legales.

SEGUNDO: Que la Ley estatutaria 1581 de 2012 tiene como objeto "desarrollar *el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política*; (...).".

Dicha ley concibe la seguridad como un principio y como un deber de obligatorio cumplimiento por parte de los Responsables y Encargados del tratamiento[3]. Adicionalmente, exige que se adopten medidas preventivas que, como su nombre lo indica, eviten o impidan la consulta, el acceso, la pérdida, la adulteración o el uso no autorizado o fraudulento de los datos personales[4].

TERCERO: Que la Ley 1581 de 2012 es aplicable a "*los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada*" o al "*tratamiento de datos personales efectuado en territorio colombiano*", con independencia de si el Responsable o el Encargado del Tratamiento se encuentra ubicado físicamente en el territorio de la República de Colombia. Por lo tanto, dicha ley aplica a cualquier operación sobre datos personales como, entre otras, la recolección, uso, almacenamiento o circulación de dicha información de personas naturales residentes o domiciliadas en la República de Colombia por parte de, entre otros, proveedores de servicios de redes sociales digitales, aunque su sede principal no se encuentre en el territorio colombiano, o parte del tratamiento se efectué fuera del mismo.

---

[1] Cfr. Ley 1581 de 2012, artículo 3°, literal g).
[2] Cfr. Ley 1581 de 2012, artículo 4°, literal g).
[3] Cfr. Artículos 4 (literal g), 17 (literal d) y 18 (literal b) de la Ley 1581 de 2012.
[4] Cfr. Artículos 4 (literal g), 17 (literal d) y 18 (literal b) de la Ley 1581 de 2012.

Buena parte del tratamiento de los datos personales se realiza a través de internet lo que facilita que desde afuera del territorio colombiano se recolecte y use la información. No obstante, ello no significa que por ese fenómeno tecnológico desaparezca la obligación de cumplir las normas locales y de respetar los derechos humanos. En este sentido, la Corte Constitucional ha precisado 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*". Recalca dicha Corporación que "*nadie podría sostener que, por tratarse de Internet, los usuarios sí pueden sufrir mengua en sus derechos constitucionales*" [5]. (Negrillas fuera del texto original).

CUARTO: Que respecto al ámbito de aplicación del artículo 2 de la Ley 1581 de 2012 en el tratamiento de los datos personales de los colombianos realizado, en parte, en un tercer país, la Corte Constitucional en Sentencia C-748 de 2011 fue clara y específica al indicar que el Régimen Colombiano de Protección de Datos Personales aplica a todo tipo de tratamiento, aunque parte del mismo ocurra precisamente fuera de las fronteras; máxime, en estos casos, que la recolección de los datos se realiza en y por medios ubicados en Colombia . Precisó la Corte:

> "*Para la Sala, esta disposición se ajusta a la Carta, pues amplía el ámbito de protección a algunos tratamientos de datos personales que ocurren fuera del territorio nacional, en virtud del factor subjetivo. En un mundo globalizado en el que el flujo transfronterizo de datos es constante, la aplicación extraterritorial de los estándares de protección es indispensable para garantizar la protección adecuada de los datos personales de los residentes en Colombia, pues muchos de los tratamientos, en virtud de las nuevas tecnologías, ocurren precisamente fuera de las fronteras. Por tanto, para la Sala se trata de una medida imperiosa para garantizar el derecho al habeas data (...)*". [6].

QUINTO: Que el artículo 19 de la Ley 1581 de 2012 ordena a la Superintendencia de Industria y Comercio (SIC), como autoridad nacional de protección de datos personales, ejercer vigilancia "*para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley*"

SEXTO: Que con sujeción a lo establecido en el artículo 21 de la Ley 1581 de 2012, le corresponde a la Superintendencia de Industria y Comercio (SIC) "*impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables*[7] *del Tratamiento y Encargados del Tratamiento a las disposiciones previstas*" en esa ley. Adicionalmente, la SIC también puede "*ordenar las medidas que sean necesarias para hacer efectivo el derecho de habeas data*".

SÉPTIMO: Que los principios rectores establecidos en la Ley 1581 de 2012 establecen las pautas mínimas que deben seguir tanto las autoridades públicas como los particulares que se relacionan con el tratamiento de datos personales[8].

El principio de legalidad[9] exige que el tratamiento de datos personales se realice de la manera que lo indique la ley y sus normas reglamentarias. Por lo tanto, el tratamiento es una actividad reglada que debe sujetarse lo establecido por la regulación de la República de Colombia.

OCTAVO: Que el principio de acceso y circulación restringida[10] le otorga el poder al titular de la información de, entre otros, decidir quiénes pueden acceder a su información personal.

NOVENO: Que el principio de seguridad[11] exige que la información sujeta a tratamiento se maneje con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad

---

[5] Todas las partes o frases señaladas entre comillas son tomadas de la sentencia C-1147 de 2001.
[6] Cfr. Corte Constitucional. Sentencia C-748/2011. M.P: Jorge Ignacio Pretelt Chaljub. Consideración 2.4.4.
[7] Ley 1581 de 2012, artículo 3°, literal e). "**Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos"
[8] Ibidem.
[9] Ley 1581 de 2012, artículo 4°, literal a). "**Principio de legalidad en materia de Tratamiento de datos:** El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen; (...)".
[10] Ley 1581 de 2012, artículo 4°, literal f). "**Principio de acceso y circulación restringida**: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley; (...).".
[11] Ley 1581 de 2012, artículo 4°, literal g). "**Principio de seguridad:** La información sujeta a Tratamiento por el responsable del tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;"

a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

DÉCIMO: Que la Corte Constitucional en Sentencia C-748 de 2011 enfatizó el deber de los proveedores de servicios de redes sociales digitales de reforzar sus medidas de seguridad para proteger la información personal de los titulares, pues, según la Corte, *"el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre"*[12].

DÉCIMO PRIMERO: Que para los fines de la presente resolución, la Dirección se permite precisar los siguientes aspectos:

11.1. Facebook Inc., es una sociedad constituida bajo las leyes del Estado de Delaware, Estados Unidos de América, con domicilio en 1601 Willow Rd, Menlo Park, California, 94025, Estados Unidos de América[13]. Mientras, Facebook Ireland Limited es una sociedad privada limitada por acciones con domicilio registrado en 4 Grand Canal Square, Gran Canal, Harbour Dublín 2, república de Irlanda[14].

11.2. Facebook Colombia SAS se encuentra registrada en la Cámara de Comercio de Bogotá, Colombia, identificada con el Nit. 900.710.525-6, con domicilio social y centro de negocios en la ciudad de Bogotá, Colombia, y fue inscrita el 4 de febrero de 2014[15].

11.3. Facebook Colombia SAS es una empresa privada de propiedad exclusiva de Facebook Global Holdings II LLC, configurándose en una situación de control, de acuerdo con el certificado de Existencia y Representación Legal de Facebook Colombia SAS[16].

11.4. Facebook Colombia SAS tiene como objeto social brindar soporte en la venta de publicidad, marketing y relaciones públicas[17] de Facebook, por ejemplo, según lo recabado en la diligencia de inspección realizada por la Dirección del 26 de marzo de 2018, *"(...) reunirse con los clientes corporativos, asesorarlos de los productos de la plataforma (...)"*[18]. Por lo tanto, Facebook Colombia SAS se constituyó para, entre otros, generarle ingresos económicos a Facebook Inc. por la venta de publicidad en Colombia; y ésta última (Facebook Inc.) ejerce actividades en Colombia, de manera real y efectiva, con y a través de Facebook Colombia SAS.

11.5. Facebook Inc., Facebook Colombia SAS, Facebook Global Holdings II y Facebook Ireland Limited forman parte del grupo de compañías de "Facebook", quienes determinan de manera conjunta los fines por los cuales y la manera en que los datos personales de los usuarios residentes y domiciliados en la República de Colombia de Facebook son tratados, para o en relación a todo el circulo de la operación de la red social de Facebook, correspondiendo a Facebook Colombia SAS, en dicho círculo, las actividades de promoción y venta de espacios publicitarios difundidos a través de la red social, que sirven, una vez más, para generarle ingresos económicos a Facebook Inc.

---

[12] Cfr. Ibídem. Consideración. 2.6.5.2.7. "**Principio de seguridad: "Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento**. De este principio se deriva entonces la responsabilidad que recae en el administrador del dato. El afianzamiento del principio de responsabilidad ha sido una de las preocupaciones actuales de la comunidad internacional, en razón del efecto "diluvio de datos", a través del cual día a día la masa de datos personales existente, objeto de tratamiento y de ulteriores transferencias, no cesa de aumentar. **Los avances tecnológicos han producido un crecimiento de los sistemas de información, ya no se encuentran sólo sencillas bases de datos, sino que surgen nuevos fenómenos como las redes sociales, el comercio a través de la red, la prestación de servicios, entre muchos otros. Ello también aumenta los riegos de filtración de datos, que hacen necesarias la adopción de medidas eficaces para su conservación. Por otro lado, el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre**. En estos términos, el **responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, por ejemplo, en materia de redes sociales, empieza a presentarse una preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. En el año 2009, el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea señaló que en los Servicios de Redes Sociales" o "SRS debe protegerse la información del perfil en el usuario mediante el establecimiento de "parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos". Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria**." (Negrillas y subrayado fuera del texto original).

[13] Folio 226.

[14] Folio 43.

[15] Folio 260.

[16] Folio 263.

[17] Folio 260.

[18] Diligencia de Inspección realizada por la Dirección de Investigación de la Protección de Datos Personales el día 26 de marzo de 2018. Folio 223-246.

11.6. Acorde con la Primera Gran Encuesta TIC/2017 "Estudio de acceso, uso y retos de las TIC en Colombia" realizada en 2017 por el Ministerio de Tecnologías de la Información y las Comunicaciones, Facebook es la red social más usada por los colombianos, ya sea en sus equipos móviles, tabletas o computadores[19].

11.7. Facebook (o FB) es un proveedor de una plataforma de servicios de comunicación en línea[20] (o proveedor de redes sociales), que permite a los usuarios construir una red social, agregar, interactuar y comunicarse con otros usuarios (o "amigos") y compartir contenido en la red social, ya sea a través de la página web, www.facebook.com, o de su Aplicación móvil complementaria.

11.8. Facebook ofrece servicios de redes sociales de forma gratuita y utiliza los datos personales que recopila para vender espacios de publicidad dirigida de terceros.

11.9. Facebook trata (o procesa) la información proporcionada directamente por el usuario (nombre, sexo, fecha de nacimiento, genero, dirección de correo electrónico, ciudad de nacimiento, intereses, educación, afiliación política, fotos, publicaciones o mensajes, etc.), información sobre el comportamiento de los usuarios en la red social ("dirección "IP", equipo, día y hora en que el usuario accede a su cuenta, navegador, etc.), información relacionada con los botones "Like" o "Me Gusta", e información creada con base en los datos que el usuario suministró o se recolectó de su actividad en Facebook.

11.10. Para los efectos de la presente resolución, cualquier referencia a "Facebook" significa la Aplicación móvil complementaria, la plataforma web y el servicio "Facebook Messenger", donde se tratan los datos personales de las personas naturales residentes o domiciliadas en la República de Colombia, así como Facebook Inc., Facebook Colombia SAS y Facebook Ireland Limited, cada uno cumpliendo su rol dentro del grupo Facebook con miras a lograr los objetivos del mismo.

11.11. El documento titulado "Política de datos"[21] y publicado por Facebook en su página web https://www.facebook.com/ establece, entre otras, lo siguiente:

> *"En esta política se describe la información que tratamos a fin de proporcionar los servicios de Facebook, Instagram y Messenger, así como de otros productos y funciones que Facebook ofrece ("Productos de Facebook" o "Productos"). Puedes obtener herramientas e información adicionales en la configuración de Facebook y de Instagram."*[22]
>
> *(...)*
>
> ***"¿Cuáles son los productos de Facebook?***
>
> *Los productos de Facebook incluyen Facebook (incluidos el navegador de la aplicación y la aplicación de Facebook para móviles), Messenger, Instagram (incluidas las aplicaciones como Direct y Boomerang), dispositivos de marca del portal, Moments, Bonfire, Facebook Mentions, Spark AR Studio, Audience Network y todas las demás funciones, aplicaciones, tecnologías, software, productos o servicios que ofrecen Facebook Inc. o Facebook Ireland Limited según nuestra Política de datos. Los productos de Facebook también incluyen las herramientas para empresas de Facebook, como plugins sociales (por ejemplo, los botones "Me gusta" o "Compartir") y nuestros SDK y API, que los propietarios y editores de sitios web, desarrolladores de aplicaciones, socios comerciales (incluidos los anunciantes) y sus clientes usan para facilitar servicios para empresas y el intercambio de información con Facebook."*[23]
>
> *(...)*
>
> "***¿Cuál es la dinámica de trabajo conjunto de las empresas de Facebook?***
>
> *Facebook e Instagram comparten infraestructura, sistemas y tecnología con otras empresas de Facebook (incluidas WhatsApp y Oculus) a fin de proporcionarte una experiencia innovadora, relevante, coherente y segura en todos los Productos de las empresas de Facebook que utilizas. Asimismo, tratamos información sobre ti en todas las empresas de Facebook con estos fines, según*

---

[19] Cfr. Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, recuperado de http://colombiatic.mintic.gov.co/602/articles-57613_Presentacion.pdf

[20] Cfr. Dictamen 5/2009 sobre las redes sociales en línea del Grupo de Trabajo del Artículo 29 (Hoy Comité Europeo de Protección de Datos), EDPB, por sus siglas en inglés, en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_es.pdf

[21] En el texto se precisa que la fecha de la última revisión del documento es: 19 de abril de 2018. Cfr. https://www.facebook.com/about/privacy/update. Última consulta: 24 de enero de 2019

[22] Cfr. https://www.facebook.com/about/privacy/update . Última consulta: 24 de enero de 2019

[23] Cfr. https://www.facebook.com/help/1561485474074139?ref=dp. Última consulta: 24 de enero de 2019

lo permitido por la legislación aplicable y de conformidad con sus condiciones y políticas. Por ejemplo, tratamos información de WhatsApp sobre cuentas que envían spam en sus servicios, de modo que podamos tomar las medidas correspondientes contra dichas cuentas en Facebook, Instagram o Messenger. Nuestro trabajo también consiste en comprender cómo usan las personas los Productos de las empresas de Facebook y cómo interactúan con ellos. Con esta finalidad, por ejemplo, recopilamos información sobre el número de usuarios únicos en distintos Productos de las empresas de Facebook."[24].

(...)

"Empresas de Facebook

"Además de los servicios que ofrecen Facebook Inc. y Facebook Ireland Ltd, Facebook posee y administra cada una de las empresas que figuran a continuación, en conformidad con sus respectivas condiciones del servicio y políticas de privacidad. Es posible que compartamos información sobre ti con las empresas de nuestro grupo para facilitar, dar asistencia e integrar sus actividades, así como para mejorar nuestros servicios. Para obtener más información sobre las prácticas de privacidad de las empresas de Facebook y cómo procesan la información de sus usuarios, consulta los siguientes enlaces:

- *Facebook Payments Inc. (https://www.facebook.com/payments_terms/privacy)*
- *Onavo (http://www.onavo.com/privacy_policy)*
- *Oculus y Oculus Ireland Limited (http://www.oculus.com/privacy/)*
- *WhatsApp Inc. y WhatsApp Ireland Limited (http://www.whatsapp.com/legal/#Privacy)*
- *Masquerade (https://www.facebook.com/msqrd/privacy)*
- *CrowdTangle (https://www.crowdtangle.com/privacy)*"[25].

(...)

"¿Cómo operamos y transferimos datos como parte de nuestros servicios internacionales?

Compartimos información de forma global, tanto internamente con las empresas de Facebook como externamente con nuestros socios y con las personas con las que te conectas y compartes contenido en todo el mundo, de conformidad con esta política. Por ejemplo, tu información puede transferirse o transmitirse a los Estados Unidos o a otros países distintos de tu lugar de residencia, así como almacenarse o procesarse en estas ubicaciones, en relación con las finalidades descritas en esta política. Estas transferencias de datos son necesarias para proporcionar los servicios descritos en las Condiciones de Facebook y las Condiciones de Instagram, así como para funcionar de forma global y proporcionarte nuestros Productos (...)".[26]

En suma, los datos personales que recolecta Facebook en Colombia o sobre personas residentes o domiciliadas en Colombia son compartidos globalmente con muchas empresas y clientes de Facebook. Esto implica que los datos personales reposan y circulan a través de una infraestructura tecnológica global ubicada y distribuida en muchos países del mundo. Facebook decide en qué países ubican su infraestructura tecnológica y las medidas de seguridad de sus millones de usuarios.

Dada la circulación transfronteriza que realiza Facebook de la información de los colombianos, las fallas de seguridad que suceden en otros países afectan o puede afectar la información de las personas residentes o domiciliadas en la República de Colombia, cuyos datos son recolectados y tratados por Facebook.

11.12. Facebook es la red social digital con mayor número de usuarios en el mundo y en la República de Colombia. En efecto, Facebook tiene aproximadamente 2.410[27] millones de usuarios en todo el mundo de los casi 4.130[28] millones de internautas. En otras palabras, Facebook trata datos personales de no menos del 58% de las personas que tienen acceso a internet.

[24] Cfr. https://www.facebook.com/about/privacy/update. Última consulta: enero 24 de 2019
[25] Cfr. https://www.facebook.com/help/111814505650678?ref=dp. Última consulta: enero 24 de 2019
[26] Cfr. https://www.facebook.com/about/privacy/update. Última consulta: enero 24 de 2019
[27] Cfr. http://www.internetlivestats.com/. Última consulta: 23 de enero de 2019
[28] Cfr. http://www.internetlivestats.com/. Última consulta: 23 de enero de 2019

En cuanto a Colombia, la cifra de usuarios de Facebook oscila entre 20[29] y 31[30] millones de personas. Si se toma este último dato y se tiene en cuenta la población colombiana (45.5 millones) según DANE[31], se puede concluir que Facebook trata los datos personales del 68% de los colombianos.[32]

Recolectar, usar, circular y tratar datos de más de 2,4 billones de personas y de 31 millones de colombianos exige que Facebook sea extremadamente responsable, diligente y profesional con la administración de tanta información de seres humanos. Por tanto, las medidas de seguridad, entre otras, deben ser las mejores y las más robustas de manera que se genere absoluta confianza a los millones de usuarios respecto de la seguridad de su información.

No obstante, ello no es así en la práctica porque en los últimos años se han detectado muy graves incidentes de seguridad, tal y como se demostrará a continuación.

DÉCIMO SEGUNDO: DE LAS FALLAS DE SEGURIDAD DE FACEBOOK

Facebook anuncia lo siguiente en la sección "Centro de Seguridad" de su página web:

> ***"Seguridad en Facebook***
>
> *(…). Queremos que todo el mundo se sienta seguro cuando utilice Facebook.*
> *Trabajamos con expertos, incluido un consejo asesor de seguridad, y recopilamos comentarios de nuestra comunidad con el objetivo de desarrollar políticas, herramientas y recursos diseñados para protegerte."*[33]

Pese a lo anterior, medios de comunicación, Facebook y las diferentes actuaciones de las autoridades de protección de datos personales (o comisionados de privacidad) han puesto de presente algunas fallas de seguridad en la plataforma de Facebook. A título de ejemplo, a continuación nos referiremos a los siguientes:

a) Del programa "Facebook Platform" y del caso Cambridge Analytica
b) Del hurto de los "tokens" para acceder a las cuentas de los usuarios de Facebook
c) Del acceso indebido a fotografías de usuarios de Facebook

12.1 Del programa "Facebook Platform" y del caso Cambridge Analytica

12.1.1. Facebook lanzó en el 2007 el programa "Facebook Platform"[34] (o "FP" por sus siglas en inglés), un extenso entorno de software que permite a terceros desarrolladores crear Aplicaciones o "Apps". Estas facilitan que los usuarios de Facebook personalicen su perfil de acuerdo a sus gustos y preferencias, por ejemplo, integrar la información de sus calendarios, horóscopos[35], y cuentas de correo electrónico con sus cuentas de Facebook, o participar en juegos con otros usuarios dentro de la misma red social.

El programa "Facebook Platform" incluye una interfaz de programación de aplicación, "API" por sus siglas en inglés, que le permite a las Aplicaciones interactuar con la plataforma de Facebook y gobierna hasta qué punto puede acceder a la amplia colección de datos de los usuarios de Facebook, entre ellos, los de los residentes y con domicilio en Colombia, incluido los datos de sus contactos o "amigos"[36].

Los desarrolladores permiten a los usuarios de Facebook acceder a sus Aplicaciones a través de un servicio disponible en "Facebook Platform" llamado "Facebook Login", el cual facilita que los

---

[29] Cfr. Facebook supera los 20 millones de usuarios en Colombia. Publicado en: http://colombia-inn.com.co/facebook-supera-los-20-millones-de-usuarios-en-colombia/ . Última consulta: 23 de enero de 2019
[30] Cfr. Latamclick (2018) Estadísticas de Facebook (América Latina) 2018 con imágenes to Share. Publicado en: https://www.latamclick.com/estadisticas-de-facebook-america-latina-2018/. Última consulta: 23 de enero de 2019
[31] Cfr. DANE. Censos y demografía. Información sobre el censo de población de 2018. Datos preliminares a noviembre de 2018. Publicado en: https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/censo-nacional-de-poblacion-y-vivenda-2018/cuantos-somos. Última consulta: 23 de enero de 2018
[32] Cítese, además, el informe publicado en el año 2018 por la organización "We are Social", titulado "Digital in 2018 in Southern America Part 1 – North". Pág. 71, en: https://www.slideshare.net/wearesocial/digital-in-2018-in-southern-america-part-1-north-86863727.
[33] Cfr. https://www.facebook.com/safety . Última consulta: 24 de enero de 2019
[34] Cfr. Revista Enter, en: https://www.enter.co/cultura-digital/redes-sociales/asi-ha-cambiado-facebook-a-traves-del-tiempo/ (Consultado en enero 20, 2019).
[35] Cfr. The Canadian Internet Policy and Public Interest Clinic (CIPPIC), en: https://cippic.ca/sites/default/files/CIPPICFacebookComplaint_29May08.pdf. Última consulta: 23 de enero de 2019).
[36] Cfr. Respuesta del 11 de abril de 2018, Folio 53.

usuarios accedan directamente a las Aplicaciones usando la cuenta de Facebook y credenciales de acceso (nombre y contraseña).

Al momento en que un usuario "visita" una Aplicación, ésta accede automáticamente a cierta información personal, considerada por Facebook como "públicamente disponible" para todos (por ejemplo: nombre, imagen de perfil, género, ciudad actual, redes, lista de amigos y páginas), sin que, según "The Electronic Privacy Information Center (EPIC)"[37], el usuario pueda controlar ese tipo de intercambio respecto de sus datos personales.

La Oficina del Fiscal General del Distrito de Columbia resumió que el programa "Facebook Platform" fue diseñado para permitir el desarrollo de Aplicaciones de terceros que se relacionan perfectamente con los usuarios de Facebook y al mismo tiempo permite a esas Aplicaciones acceder a una gran cantidad de datos personales recolectados de los usuarios de Facebook[38].

12.1.2. El 17 de marzo de 2018, el diario británico "The Guardian", en colaboración con los periódicos "The New York Times" y "The Observer", informó que Cambridge Analytica había utilizado indebidamente los datos personales de más de 50 millones usuarios de Facebook[39]; información que había sido obtenida a través de la aplicación "thisyourdigitallife", que fue desarrollada por el Dr. Aleksandr Kogan[40].

La información involucrada hacía referencia a los nombres completos, edad, educación, intereses, historia laboral, cumpleaños, "like" o "me gusta", localización física, fotos, estatus social, afiliaciones políticas y religiosas de los usuarios de Facebook[41]. Y, según la demanda que radicó la Oficina del Fiscal del Estado de Illinois contra Facebook, se crearon perfiles psicográficos (psychographic profiles[42]) de los usuarios[43], permitiendo a Cambridge Analytica influenciar de manera confiable sobre ellos y manipular su comportamiento, con las llamadas "noticias falsas" en varias plataformas, incluyendo Facebook[44].

12.1.3. El 21 de marzo de 2018[45], el señor Mark Zuckerberg, fundador y director ejecutivo de Facebook, reconoció que el escándalo generado por el uso ilegal de los datos personales de los

---

[37] Cfr. Electronic Privacy Information Center (EPIC), en: https://epic.org/privacy/inrefacebook/. Última consulta: 23 de enero de 2019.
[38] Cfr. The Office of the Attorney General for the District of Columbia, copia de la demanda en: http://oag.dc.gov/sites/default/files/2018-12/Facebook-Complaint.pdf
[39] "The Guardian", en: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Folios 1 al 6.
[40] El señor "Aleksandr Kogan is a professor at Cambridge University in England. He created a Facebook application with a questionnaire asking certain personal questions. The app gave the developers permission to use the profiles of users that downloaded the app, and also all of their "Facebook friends", which is how data was collected from 87 million users globally. The Ripon platform is a software created by AIQ which was used by Cambridge Analytica during the 2016 American presidential election, first for Ted Cruz, and subsequently for Donald Trump. It allegedly used the profiles of American Facebook users collected by Dr. Kogan and sold to Cambridge Analytica". The Standing Committee on Access to Information, Privacy and Ethics (The House of Commons of Canada). Reporte: "ADDRESSING DIGITAL PRIVACY VULNERABILITIES AND POTENTIAL THREATS TO CANADA'S DEMOCRATIC ELECTORAL PROCESS"- Cita 11, pág. 5. En: https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf
[41] Cfr. Craig Timberg, Tony Romm, and Elizabeth Dwoskin, U.S. and European Officials Question Facebook's Protection of Personal Data, Washington Post, en: https://www.washingtonpost.com/business/economy/us-and-european-officials-question-facebooks-protection-ofpersonal-data/2018/03/18/.
[42] Cr. "(…) 58. Broadly speaking, psychographic profiling is a marketing tool that combines a detailed psychological analysis of an individual using various data points about their interests, activities, opinions, and motivations. These data points can then be layered on top of demographic information such as race, gender, and age. 59. Psychographic profiling tools—including Cambridge Analytica's—can combine assessments of a person's innate personality characteristics with predictions of, for instance, their voting behavior, to create hyper-focused predictions about not only what people will do, but what will motivate them to do it. 60. The personality traits that Cambridge Analytica has claimed can be predicted through psychographic profiling included, most importantly, a person's OCEAN ratings, a common personality type classification method that looks at five factors: Openness, Conscientiousness, Extraversion, Agreeableness, and Neuroticism. In addition, Cambridge Analytica has claimed to be able to predict—based on the data it possesses—an individual's age, political views, religion, profession, whether they are fair-minded or suspicious of others, and even (ironically) whether they prefer to disclose facts about themselves to others or value their privacy. 61. According to Cambridge Analytica, this allowed its clients to bypass individuals' cognitive defenses by appealing directly to their emotions, using increasingly segmented and sub-grouped personality type designations and precisely targeted messaging based on those designations.(…)". Páginas 16 y 17, en el caso: "PEOPLE OF THE STATE OF ILLINOIS, ex rel. Kimberly M. Foxx, State's Attorney of Cook County, Illinois, Plaintiff, v. FACEBOOK, INC., a Delaware corporation, SCL GROUP LIMITED, a United Kingdom private limited company, and CAMBRIDGE ANALYTICA LLC, a Delaware limited liability Company", en: https://www.cookcountystatesattorney.org/sites/default/files/files/documents/cook_county_sao-facebook_cambridge_analytica_complaint.pdf
[43] Cfr. Caso: PEOPLE OF THE STATE OF ILLINOIS, ex rel. Kimberly M. Foxx, State's Attorney of Cook County, Illinois, Plaintiff, v. FACEBOOK, INC., a Delaware corporation, SCL GROUP LIMITED, a United Kingdom private limited company, and CAMBRIDGE ANALYTICA LLC, a Delaware limited liability Company, en: https://www.cookcountystatesattorney.org/sites/default/files/files/documents/cook_county_sao-facebook_cambridge_analytica_complaint.pdf
[44] Cfr. Ibídem.
[45] Cfr. (i) Periódico ABC de España, en: https://www.abc.es/tecnologia/redes/abci-mark-zuckerberg-investigaremos-todas-aplicaciones-tuvieron-acceso-grandes-cantidades-informacion-201803212058_noticia.html Última consulta: 20 de enero de 2019.

usuarios era una ruptura de la confianza entre el Dr. Aleksandr Kogan, Cambridge Analytica y Facebook, pero también una ruptura de la confianza entre Facebook y la gente que comparte sus datos con esa red social.

Él anunció, entre otras acciones, que: (i) se revisará a las Aplicaciones que tengan acceso a gran cantidad de datos de los usuarios, incluyendo una auditoria completa a cualquier Aplicación con actividad sospechosa; (ii) se restringirá el acceso a los datos personales sin consentimiento; (iii) se reducirá la cantidad de datos personales solicitados por los desarrolladores de Aplicaciones; (iv) se exigirá la suscripción de un contrato para que cada Aplicación pueda acceder a las publicaciones de un usuario y cualquier dato privado; y (v) se implementará una herramienta en la página del perfil que les permita a los usuarios revocar el consentimiento para el uso de los datos por parte de las Aplicaciones.

12.1.4. El 21 de marzo de 2018[46], el Grupo de Trabajo del Artículo 29 (Hoy Comité Europeo de Protección de Datos) publicó el siguiente comunicado de prensa:

> *"Como una regla, los datos personales no pueden ser usados sin una transparencia total sobre cómo ellos se están utilizando y con quién se están compartiendo. Esto, por lo tanto, es una acusación muy seria con consecuencias para los derechos de los datos personales de los individuos y del proceso democrático. ICO, la autoridad británica del Reino Unido está llevando una investigación sobre el caso" de Facebook - Cambridge Analytica."*

12.1.5. El 26 de marzo de 2018[47], la Comisión Federal de Comercio de los Estados Unidos -The Federal Trade Commission- anunció que esa comisión había abierto una investigación contra

---

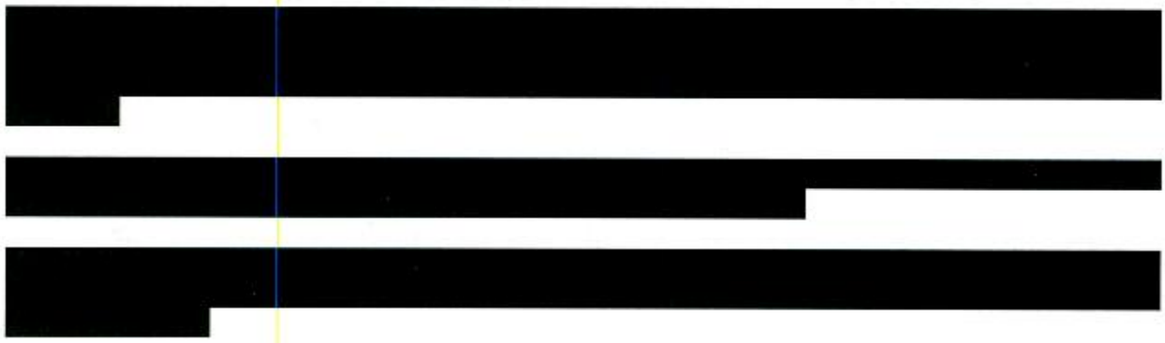
y, (ii) Mark Zuckerberg, en: https://www.facebook.com/zuck/posts/10104712037900071 (Última consulta: 23 de enero de 2019). Cita el comunicado de prensa del Señor Zuckerberg: I want to share an update on the Cambridge Analytica situation -- including the steps we've already taken and our next steps to address this important issue. We have a responsibility to protect your data, and if we can't then we don't deserve to serve you. I've been working to understand exactly what happened and how to make sure this doesn't happen again. The good news is that the most important actions to prevent this from happening again today we have already taken years ago. But we also made mistakes, there's more to do, and we need to step up and do it. Here's a timeline of the events: In 2007, we launched the Facebook Platform with the vision that more apps should be social. Your calendar should be able to show your friends' birthdays, your maps should show where your friends live, and your address book should show their pictures. To do this, we enabled people to log into apps and share who their friends were and some information about them. In 2013, a Cambridge University researcher named Aleksandr Kogan created a personality quiz app. It was installed by around 300,000 people who shared their data as well as some of their friends' data. Given the way our platform worked at the time this meant Kogan was able to access tens of millions of their friends' data. In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the data apps could access. Most importantly, apps like Kogan's could no longer ask for data about a person's friends unless their friends had also authorized the app. We also required developers to get approval from us before they could request any sensitive data from people. These actions would prevent any app like Kogan's from being able to access so much data today. In 2015, we learned from journalists at The Guardian that Kogan had shared data from his app with Cambridge Analytica. It is against our policies for developers to share data without people's consent, so we immediately banned Kogan's app from our platform, and demanded that Kogan and Cambridge Analytica formally certify that they had deleted all improperly acquired data. They provided these certifications. Last week, we learned from The Guardian, The New York Times and Channel 4 that Cambridge Analytica may not have deleted the data as they had certified. We immediately banned them from using any of our services. Cambridge Analytica claims they have already deleted the data and has agreed to a forensic audit by a firm we hired to confirm this. We're also working with regulators as they investigate what happened. This was a breach of trust between Kogan, Cambridge Analytica and Facebook. But it was also a breach of trust between Facebook and the people who share their data with us and expect us to protect it. We need to fix that. In this case, we already took the most important steps a few years ago in 2014 to prevent bad actors from accessing people's information in this way. But there's more we need to do and I'll outline those steps here: First, we will investigate all apps that had access to large amounts of information before we changed our platform to dramatically reduce data access in 2014, and we will conduct a full audit of any app with suspicious activity. We will ban any developer from our platform that does not agree to a thorough audit. And if we find developers that misused personally identifiable information, we will ban them and tell everyone affected by those apps. That includes people whose data Kogan misused here as well. Second, we will restrict developers' data access even further to prevent other kinds of abuse. For example, we will remove developers' access to your data if you haven't used their app in 3 months. We will reduce the data you give an app when you sign in -- to only your name, profile photo, and email address. We'll require developers to not only get approval but also sign a contract in order to ask anyone for access to their posts or other private data. And we'll have more changes to share in the next few days. Third, we want to make sure you understand which apps you've allowed to access your data. In the next month, we will show everyone a tool at the top of your News Feed with the apps you've used and an easy way to revoke those apps' permissions to your data. We already have a tool to do this in your privacy settings, and now we will put this tool at the top of your News Feed to make sure everyone sees it. Beyond the steps we had already taken in 2014, I believe these are the next steps we must take to continue to secure our platform. I started Facebook, and at the end of the day I'm responsible for what happens on our platform. I'm serious about doing what it takes to protect our community. While this specific issue involving Cambridge Analytica should no longer happen with new apps today, that doesn't change what happened in the past. We will learn from this experience to secure our platform further and make our community safer for everyone going forward. I want to thank all of you who continue to believe in our mission and work to build this community together. I know it takes longer to fix all these issues than we'd like, but I promise you we'll work through this and build a better service over the long term."

[46] Cfr. Grupo de Trabajo del Artículo 29 de la Unión Europea, en: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=617458. "Cambridge Analytica – reaction Andrea Jelinek, Chair of the Article 29 Working Party "As ea rule personal data cannot be used without full transparency on how it is used and with whom it is shared. This is therefore a very serious allegation with far-reaching consequences for data protection rights of individuals and the democratic process. ICO, the UK´s data protection authority, is conducting the investigation into this matter. As Chair of the Article 29 Working Party, I fully support their investigation. The Members of the Article 29 Working Party will work together in this process." (Traducción no oficial).

[47] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection

Facebook por el escándalo de Cambridge Analytica, con el fin de determinar si Facebook había incumplido la orden emitida en el 2011 (ver numeral 13.2).

12.1.6. El 11 de abril de 2018[48], Facebook Ireland Limited le informó a esta Dirección **que la falla de seguridad sufrida por Facebook, en el caso de Cambridge Analytica, afectó la información personal de alrededor de 146,697 personas en Colombia**. Se cita su respuesta:



12.1.7. El 14 de mayo de 2018[49], Facebook emitió un comunicado sobre los hallazgos encontrados por su equipo de trabajo respecto del acceso a grandes cantidades de información personal de sus usuarios por parte de los terceros desarrolladores de las Aplicaciones. Cita el comunicado de prensa lo siguiente:

> *"A continuación, una actualización sobre el estado de la investigación y la auditoría de las aplicaciones que Mark Zuckerberg prometió el 21 de marzo.*
>
> *Como Mark explicó, Facebook investigará todas las aplicaciones que tuvieron acceso a grandes cantidades de información antes de que cambiáramos nuestras políticas en 2014, lo que redujo significativamente la posibilidad de obtener datos en la plataforma. También dejó en claro que cualquier aplicación individual que nos generara preocupación sería auditada, y si rechazara la revisión o no consiguiera superarla, quedaría excluida de Facebook.*
> *El proceso de investigación está en pleno desarrollo y consta de dos fases. Una primera revisión exhaustiva para identificar las aplicaciones que tuvieron acceso a datos en Facebook y, en caso de que surgieran dudas, haremos entrevistas, conduciremos solicitudes de información (SDF) -que contemplan una serie detallada de preguntas sobre la aplicación y los datos a los que accedía- y auditorías, que pueden incluir inspecciones en el lugar.*
>
> *Tenemos grandes equipos de expertos, tanto interna como externamente, que trabajan para culminar las investigaciones lo más rápido posible. Hasta la fecha, miles de aplicaciones han sido revisadas y cerca de 200 fueron suspendidas y serán sometidas a una indagatoria exhaustiva para determinar si efectivamente utilizaron los datos en forma inapropiada. Donde sea que encontremos evidencia de que esas u otras aplicaciones hicieron un mal uso de la información, serán prohibidas y sus casos notificados en este sitio web. De esa manera, las personas podrán saber si ellas o sus amigos instalaron una aplicación que usó datos en forma incorrecta antes del 2015, de la misma manera en que ocurrió con Cambridge Analytica.*
>
> *Aún queda mucho trabajo por delante para identificar todas las aplicaciones involucradas en malas prácticas en el uso de uso de datos personales en Facebook y sabemos que llevará tiempo. Estamos invirtiendo fuertemente para asegurarnos que la investigación sea lo más completa y oportuna posible. Los mantendremos informados de nuestros avances.".*

12.1.8. Finalmente, el 24 de octubre de 2018[50], la Oficina del Comisionado de Información de Gran Bretaña (ICO) impuso una sanción monetaria de 500.000 libras esterlinas contra Facebook por el uso ilegal de los datos personales de los usuarios de Facebook, residentes y ciudadanos domiciliados en Gran Bretaña, por parte de Cambridge Analytica (ver punto 13.3).

12.2. Del hurto de "tokens" de acceso a las cuentas de los usuarios Facebook

[48] Respuesta del 11 de abril de 2018. Folios 53 y 54.
[49] Cfr. Facebook, "Una Actualización sobre la investigación y la Auditoria de nuestras aplicaciones", en: https://ltam.newsroom.fb.com/news/2018/05/una-actualizacion-sobre-la-investigacion-y-la-auditoria-de-nuestras-aplicaciones/
[50] Cfr. The Information Comissioner's Office, ICO, en: https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf

El 25 de septiembre de 2018[51], con una actualización del 2[52] y 12 de octubre de 2018[53], respectivamente, Facebook informó que su equipo de ingenieros detectó otro incidente de seguridad que afectó por lo menos 40 millones de cuentas. Cita el comunicado de prensa lo siguiente:

> "*Nuestra investigación está aún en una fase inicial. Pero es evidente que los atacantes explotaron una vulnerabilidad en el código de Facebook, que impactó a la herrmienta (sic) "Ver Como", que permite a los usuarios mirar cómo lucen sus propios perfiles desde la óptica de otras personas. Esto les permitió robar "tokens" de acceso a Facebook, que luego podrían ser empleadas para tomar el control de cuentas de usuarios. Los "tokens" de acceso son el equivalente a llaves digitales que mantienen a las personas conectadas a Facebook y evitan que tengan que reingresar su clave cada vez que quieren usar la plataforma.*
>
> *Estas son las medidas que ya tomamos. Primero, reparamos la vulnerabilidad y reportamos el caso a las autoridades.*
>
> *Segundo, reiniciamos los tokens de acceso de las casi 50 millones de cuentas que sabemos que fueron afectadas para garantizar su seguridad. Además, tomamos la medida de inhabilitar los tokens de acceso de otras 40 millones de cuentas que usaron la funcionalidad "Ver Como" en el último año. Como resultado, cerca de 90 millones de personas deberán ahora reconectarse a Facebook o alguna de las aplicaciones a las que se accede utilizando Facebook. Luego de reconectarse, los usuarios recibirán una notificación en su News Feed, explicando lo sucedido.*
>
> *Tercero, desactivamos temporalmente la herramienta "Ver Como", mientras realizamos un chequeo exhaustivo de la seguridad.*
>
> *Este ataque aprovechó una compleja interacción entre múltiples aspectos de nuestro código. Fue originado a un cambio que hicimos del código de nuestra herramienta para subir videos en julio de 2017, que impactó la funcionalidad "Ver Como". Los atacantes identificaron esta vulnerabilidad y la utilizaron para conseguir un token de acceso, para después emplear esa cuenta como pívot para acceder a otras cuentas y robar más tokens.*
>
> *Nuestra investigación recién comienza y aún deberemos determinar si las cuentas afectadas fueron abusadas o si los atacantes lograron acceder a algún tipo de información. Tampoco sabemos quién está detrás de estos ataques o dónde se encuentran. Estamos trabajando a tiempo completo para obtener todos esos detalles y actualizaremos este blogpost cuando tengamos nueva información para compartir. Adicionalmente, si detectamos que más cuentas fueron afectadas, reiniciaremos inmediatamente sus tokens.*". (Subrayado y comillas fuera del texto original).

El 3 de octubre de 2018[54], la autoridad de protección de datos de Irlanda (The Data Protection Commission of Ireland) anunció que había iniciado una investigación contra Facebook relacionada con la anterior falla de seguridad, la cual les fue notificada por Facebook el 28 de septiembre de 2018.

12.3. Del acceso indebido a fotografías de usuarios de Facebook por falla en el "Photo API" de Facebook

El 14 de diciembre de 2018[55], el señor Tomer Bar, Director de Ingeniería de Facebook, informó que una falla en el "Photo API" generó que los terceros desarrolladores de Aplicaciones, (1.500 Aplicaciones construidas por 876 desarrolladores), accedieran a gran cantidad de fotografías de aproximadamente 5.6 millones de usuarios, durante el periodo de 12 días entre el 13 al 25 de septiembre de 2018; Aplicaciones a las cuales no se les había concedido el acceso.

---

[51] Cfr. Facebook, "Una Actualización en materia de Seguridad", en: https://ltam.newsroom.fb.com/news/2018/09/una-actualizacion-en-materia-de-seguridad/

[52] Cfr. Facebook, "Actualización sobre Facebook Login", en: https://ltam.newsroom.fb.com/news/2018/10/actualizacion-sobre-facebook-login/

[53] Cfr. Facebook, "Una Actualización en materia de Seguridad", en: https://ltam.newsroom.fb.com/news/2018/10/actualizacion-sobre-el-incidente-de-seguridad/

[54] Cfr. The Data Protection Commission of Ireland, en: https://www.dataprotection.ie/docs/EN/03-10-2018-Facebook-Data-Breach-Commencement-of-Investigation/i/1787.htm. Cita el comunicado de prensa: "The Irish Data Protection Commission (DPC) has today, 3 October 2018, commenced an investigation under Section 110 of the Data Protection Act 2018 into the Facebook data breach for which notification was received by the DPC on Friday 28 September. In particular, the investigation will examine Facebook's compliance with its obligation under the General Data Protection Regulation to implement technical and organizational measures to ensure the security and safeguarding of the personal data it processes. Facebook has informed the DPC that their internal investigation is continuing and that the company continues to take remedial actions to mitigate the potential risk to users.".

[55] Cfr. TechCrunch, "Facebook bug exposed up to 6.8M users' unposted photos to apps", en: https://techcrunch.com/2018/12/14/facebook-photo-bug/ (Consultado en enero 22 de 2019), y Facebook, Notifying "our Developer Ecosystem about a Photo API Bug", en: https://developers.facebook.com/blog/post/2018/12/14/notifying-our-developer-ecosystem-about-a-photo-api-bug/ (Consultado en enero 22 de 2019).

La falla de seguridad afectó fotos publicadas y no publicadas por los usuarios de Facebook.

Frente a este caso, el 17 de diciembre de 2018[56], la DPC anunció la apertura de otra investigación contra Facebook relacionada con el número de reportes (o notificaciones) de incidentes desde la entrada en vigencia del Reglamento General de Protección de Datos de la Unión Europea (UE RGPD).

DÉCIMO TERCERO: Que para los fines de la presente resolución, esta Dirección también considera importante hacer referencia a los diferentes estudios, investigaciones, demandas, recomendaciones, órdenes y sanciones emitidas por las diferentes autoridades nacionales de protección de datos (o comisionados de privacidad), la Oficina del Fiscal General para el Distrito de Columbia de los Estados Unidos y la Casa de los Comunes del Parlamento Canadiense, quien citó el debate realizado en la Casa de los Comuniones de Gran Bretaña y el Congreso de los Estados Unidos[57], contra Facebook, incluida la orden de acuerdo de consentimiento con la Comisión Federal de Comercio de los Estados Unidos.

13.1. The Data Protection Commission of Ireland (DPC)

El 21 de diciembre de 2011[58] y el 21 de septiembre de 2012[59], respectivamente, la Comisión de Protección de Datos de Irlanda ("The Data Protection Commission of Ireland"), en adelante la "DPC" por sus siglas en inglés, publicó los resultados de una auditoría realizada a Facebook Irlanda, subsidiaria de Facebook Inc. (EE.UU.), con el fin de evaluar el cumplimiento de Facebook con la regulación irlandesa de protección de datos y con la Directiva 95/46/CE de la Unión Europea (derogada por el Reglamento General de Protección de Datos). En el informe, se señala lo siguiente:

- Facebook permite:
  (i) que los desarrolladores de terceros creen Aplicaciones que se integran en su plataforma.
  (ii) la integración con otros sitios web (por ejemplo, a través de complementos sociales o "social plugins") e integración con Aplicaciones móviles.
  (iii) que los desarrolladores de Aplicaciones accedan a los datos de los usuarios que descargan esas aplicaciones, incluyendo aquella información personal de sus "amigos".
- El "token" de acceso concedido a una primera Aplicación podría ser transferido entre Aplicaciones, permitiendo que, por ejemplo, una segunda Aplicación pueda acceder a la información que el usuario no había consentido mediante el "token" otorgado a la primera Aplicación.
- Las políticas y procedimientos implementados no estaban documentados formalmente por parte de Facebook.
- Se recomendó a Facebook:
  (i) realizar un monitoreo constante para garantizar que no haya abuso por parte sus empleados frente al acceso a la información de los usuarios, por ejemplo, a través de los restablecimientos de contraseña inapropiados de la cuenta de un usuario.
  (ii) ser más estricto en la política de roles y responsabilidades para evitar el acceso indiscriminado por parte de su personal a los datos de los usuarios de Facebook.
  (iii) adoptar medidas adicionales para prevenir que las Aplicaciones de terceros puedan acceder a más datos personales que aquellos permitidos por el usuario, cuando la persona descarga esas Aplicaciones en Facebook.

El 3 de octubre de 2018[60], la DPC anunció que esa entidad había iniciado una investigación contra Facebook relacionada con un incidente de seguridad ocurrido y notificado por Facebook a dicha entidad el 28 de septiembre de 2018. Dicha investigación se inició, según el comunicado de prensa,

---

[56] Cfr. The Data Protection Commission of Ireland https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-facebook

[57] Citese, además, las audiencias celebradas en el Congreso de los Estados Unidos, entre ellas: (i) "Cambridge Analytica and Other Facebook Partners: Examining Data Privacy Risks", en: https://www.commerce.senate.gov/public/index.cfm/hearings?ID=01312BF5-D711-4284-AF56-04E5D77EFC7E; (ii) "Facebook, Social Media Privacy, and the Use and Abuse of Data", en https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data (Consultado en enero 23 de 2019).

[58] Cfr. The Data Protection Commission of Ireland, en: https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf

[59] Cfr. The Data Protection Commission of Ireland, en: https://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf

[60] Cfr. The Data Protection Commission of Ireland , en: https://www.dataprotection.ie/docs/EN/03-10-2018-Facebook-Data-Breach-Commencement-of-Investigation/i/1787.htm

para determinar si Facebook cumple (o no) con el Reglamento General de Protección de Datos de la Unión Europea (UE RGPD). En particular, si cuenta (o no) con las medidas técnicas y organizativas para garantizar la seguridad y la protección de los datos personales que procesa de sus usuarios.

El 17 de diciembre de 2018[61], la DPC anunció que esa entidad había iniciado otra investigación contra Facebook relacionada con el número de reportes (o notificaciones) de incidentes desde la entrada en vigencia del Reglamento General de Protección de Datos de la Unión Europea (UE RGPD), incluido el último incidente sucedido a Facebook.

13.2. The Federal Trade Commission (FTC)

El 11 de noviembre de 2011[62], la Comisión Federal de Comercio de los Estados Unidos ("The Federal Trade Commission"), en adelante la "FTC" por sus siglas en inglés, emitió una orden preliminar contra Facebook y el 27 de julio de 2012[63] aprobó la orden definitiva de acuerdo por consentimiento. La FTC le ordenó a Facebook lo siguiente:

- Evitar realizar falsas declaraciones sobre privacidad o seguridad de la información personal de los usuarios.
- Obtener el consentimiento expreso y afirmativo de los usuarios antes de promulgar cambios que anulen sus preferencias de privacidad.
- Informar a los usuarios de Facebook, con antelación al momento que dicha empresa comparta la información de sus usuarios con terceras partes, lo siguiente: (i) la categoría de información que será compartida con los terceros; (ii) la identidad o categorías específicas de dichos terceros; y, (iii) que dicho intercambio supera las restricciones impuestas por las configuraciones de privacidad por defecto para el usuario.
- Solicitar el consentimiento expreso del usuario antes de que Facebook comparta la información personal del mismo con terceros.
- Realizar los procesos necesarios para garantizar que la información de sus usuarios no pueda ser accedida por terceras partes después de un periodo de tiempo razonable, sin exceder los 30 días, desde el momento en que el usuario haya eliminado dicha información, o eliminada su cuenta.
- Establecer, implementar y mantener un programa de privacidad con miras a: (i) abordar los riesgos en privacidad relacionados con el desarrollo y la gestión de productos y servicios nuevos y existentes para los usuarios; y, (ii) proteger la privacidad y confidencialidad de la información procesada. El programa debe mantenerse por escrito, contener controles y procedimientos apropiados para el tamaño y complejidad de Facebook, la naturaleza y ámbito de las actividades de Facebook y la sensibilidad de la información.
- Realizar una auditoria inicial, así como, obtener evaluaciones y reportes bianuales por parte de un profesional independiente que permitan demostrar que los controles de privacidad implementados por Facebook garantizan la seguridad y confidencialidad de la información procesada.

El 26 de marzo de 2018[64], la FTC anunció que la Comisión había abierto una investigación contra Facebook por el escándalo de Cambridge Analytica y así determinar si Facebook había incumplido (o no) la orden emitida en el 2011[65].

13.3. The Information Commissioner's Office (ICO)

El 17 de mayo de 2017[66], la Oficina del Comisionado de Información de Gran Bretaña (The Information Commissioner's Office, ICO), en adelante "ICO" por sus siglas en inglés, anunció la apertura de una investigación respecto del uso de los datos personales de los usuarios de Facebook

---

[61] Cfr. The Data Protection Commission of Ireland https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-facebook

[62] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf

[63] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf

[64] Cfr. The Federal Trade Commission (FTC), en: https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection

65 Citese, en este punto, el link de la audiencia: "Facebook, Social Media Privacy, and the Use and Abuse of Data", llevada a cabo en el Congreso de los Estados Unidos de América, en https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data

[66] Cfr. The Information Comissioner's Office, ICO, en: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/05/blog-the-information-commissioner-opens-a-formal-investigation-into-the-use-of-data-analytics-for-political-purposes/

por parte de campañas políticas, partidos, compañías de medios sociales y otros actores comerciales.

El 24 de octubre de 2018[67], ICO anunció que esa autoridad impuso una sanción monetaria de 500.000 libras esterlinas contra Facebook bajo la sección 5ª del "Data Protection Act 1998". ICO encontró lo siguiente:

- Facebook permitió que la Aplicación, conocida como 'thisisyourdigitallife', operada por el Dr. Aleksandr Kogan/Global Science Research Limited (GSP) y descargada por sus usuarios a través de Facebook, se utilizará para crear perfiles con fines políticos: Este uso, según la decisión adoptada, escapaba de la "expectativa razonable" de los usuarios (o "data subjects" por sus siglas en inglés).
- Facebook permitió que la Aplicación accediera a:
  (i) la información de los usuarios que la habían descargado, los amigos de dichos usuarios e individuos que intercambiaron mensajes electrónicos con dichos usuarios, sin que, en esos casos, se les hubiere informado que su información sería recolectada por la Aplicación.
  (ii) una cantidad de datos que no eran necesarios para su funcionamiento.
- Facebook permitió que la Aplicación
  (i) compartiera los datos personales recolectados con terceros, para fines políticos sin que, según la decisión, se hubiera informado de dicha divulgación o sin darle la oportunidad al usuario para otorgar su consentimiento.
  (ii) retuviera la información de los usuarios y amigos de los usuarios, sin que, según la decisión, Facebook las hubiera requerido para que procedieran a eliminar la información personal procesada.
- Facebook no adoptó las medidas necesarias para asegurar que la Aplicación cumpliera con su política de privacidad y el contrato suscrito entre Facebook y ella, entre otras: revisar que los términos y condiciones de la Aplicación cumpliera con sus políticas de privacidad.
- Facebook tampoco estableció un sistema de monitoreo para determinar si la Aplicación estaba siendo operada de una manera consistente con sus políticas de privacidad y el contrato.
- Facebook falló en adoptar las medidas técnicas y administrativas apropiadas para evitar el acceso y procesamiento no autorizado de los datos personales de los usuarios, amigos de los usuarios e individuos con los que los usuarios de la Aplicación habían intercambiados mensajes; esto incluso con posterioridad a la fecha en que Facebook tuvo conocimiento sobre el incidente que afectó a los datos personales de sus usuarios.

13.4. The Commission Nationale de l'informatique et des libertés (CNIL)

El 16 de mayo de 2017,[68] la Comisión Nacional de Informática y de las Libertades de Francia (La Commission Nationale de l'informatique et des libertés, CNIL), en adelante CNIL por sus siglas en francés, informó que esa entidad había sancionado a Facebook por incumplir la regulación francesa en protección de datos personales.

La CNIL encontró que Facebook:
(i) procesaba una gran cantidad de datos personales para fines de publicidad dirigida, sin tener una base legal para hacerlo; y,
(ii) recolectaba la información relacionada con el comportamiento de los usuarios tan pronto como ellos navegaban en sitios web de terceros, que incluyen "plug-ins sociales", a través de la cookie denominada "datr", sin obtener, para ese tipo específico de tratamiento, el consentimiento de los usuarios.

13.5. The Dutch Data Protection Authority (Dutch DPA)

El 23 de febrero de 2017[69], la Autoridad de Protección de Datos de los Países Bajos (Autoriteit Persoonsgegevens), en adelante la "Dutch DPA" por sus siglas en inglés, encontró que Facebook incumplió la regulación holandesa en protección de datos personales.

---

[67] Cfr. The Information Comissioner's Office, ICO, en: https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf
[68] Cfr. La Commission nationale de l'informatique et des libertés (CNIL), en: https://www.cnil.fr/en/facebook-sanctioned-several-breaches-french-data-protection-act ¬ https://www.cnil.fr/en/common-statement-contact-group-data-protection-authorities-netherlands-france-spain-hamburg-and
[69] Cfr. Autoriteit Persoonsgegevens, en: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_facebook_february_23_2017.pdf

La Dutch DPA concluyó que:

- Facebook no:
  (i) proporcionaba la suficiente información a sus usuarios acerca del uso de su información personal con fines de publicidad.
  (ii) informaba a los usuarios sobre las diferentes categorías de información personal procesadas con fines de publicidad.
  (iii) comunicaba a sus usuarios que éste procesa datos de naturaleza sensible recolectados de los perfiles sin obtener, en esos casos, su explicito consentimiento.

- Facebook informaba a los anunciantes que dicha compañía procesa el dato de localización de los "amigos" de los usuarios para fines de publicidad, pero omitía informar a los usuarios acerca de ello.
- Facebook omitió informar adecuadamente a los usuarios que, basada en su nueva política de privacidad, esa compañía podía rastrear el comportamiento de navegación web y el uso de Aplicaciones fuera de Facebook y usar estos datos con fines publicitarios (Facebook recolecta dicha información al momento en que un usuario visita una página web o usa una Aplicación que contiene el botón "like", u otra interacción con Facebook, incluso si el usuario no le da clic a ese botón o si el usuario se ha desconectado del servicio).
- Facebook proporcionaba información incorrecta en sus términos y condiciones, así como, en el banner de cookies, acerca del significado del consentimiento para el uso de los datos personales para fines de publicidad.
- Facebook avisaba a sus usuarios, de manera incorrecta e incompleta, sobre los mecanismos diseñados para controlar la publicidad dirigida y las consecuencias de ejercer las diferentes opciones del mecanismo "opt-out".

13.6. The Office of the Privacy Commissioner of Canada (OPC) y The Standing Committee on Access to Information, Privacy and Ethics

El 16 de julio de 2009[70], la Oficina del Comisionado de Privacidad de Canadá, en adelante la "OPC" por sus siglas en inglés, publicó su informe final en la investigación adelantada contra Facebook por el posible incumplimiento de la "Personal Information Protection and Electronic Documents Act", en adelante PIPEDA por sus siglas en inglés.

La OPC encontró los siguientes hallazgos:

- La recolección del dato relacionado con la fecha de nacimiento es aceptable como una condición para la prestación del servicio, desde que su uso sea apropiado. Sin embargo, Facebook no fue claro en explicar dichas finalidades.
- Las configuraciones de privacidad predeterminadas son aceptables, siempre y cuando se cumplan con las "expectativas de razonabilidad" de los usuarios. Facebook no lo cumple en dos casos: álbumes de fotos (configurados en "Todos") y búsqueda (consentimiento para que los motores de búsqueda puedan buscarlos).
- Facebook no proporciona suficiente información a los usuarios respecto de las configuraciones predeterminadas de privacidad y las implicaciones de no modificarlas.
- Los usuarios no pueden ejercer el mecanismo "opt-out" respecto a la publicidad, ya que los ingresos de publicidad se requieren para ejecutar el sitio (que es gratuito para los usuarios).
- Facebook no está informando a los usuarios del uso de sus datos personales para fines publicitarios.
- **Facebook tiene medidas de seguridad <u>inadecuadas</u> para restringir efectivamente a aquellos desarrolladores de Aplicaciones el acceso a la información del perfil de los usuarios, así como, a la información personal de sus amigos en línea**.
- Facebook no estaba obteniendo el consentimiento informado de los usuarios para la divulgación de su información personal a los desarrollares de Aplicaciones, ya sea cuando éstos o sus amigos agregan (o descargan) las Aplicaciones.

La OPC recomendó a Facebook adoptar las siguientes medidas para cumplir con la regulación canadiense (PIPEDA):

---

[70] Cfr. The Office of the Privacy Commissioner of Canada (OPC), en: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-008/

- Informar claramente a los usuarios sobre la recolección del dato relacionado con su fecha de nacimiento, las razones y los propósitos de su uso.
- Evaluar si los perfiles de los usuarios pueden, por defecto, ser inaccesibles, para los motores de búsqueda.
- Cambiar las configuraciones por defecto para los álbumes de fotos.
- Proporcionar un enlace a las configuraciones de privacidad, acompañado por un enlace que incluya: (i) los propósitos de dichas configuraciones; (ii) las configuraciones que Facebook ha pre-establecido; y, (iii) las configuraciones que pueden ser cambiadas por los usuarios.
- **Implementar las medidas necesarias para**:
  - **(i) limitar el acceso por parte de los desarrolladores de Aplicaciones a los datos de los usuarios, que no son necesarios para el funcionamiento de las mismas.**
  - **(ii) informar a los usuarios sobre la información específica que requiere una Aplicación y con qué propósito su información será utilizada por ellas.**
  - **(iii)solicitar el consentimiento expreso de los usuarios al acceso del desarrollador de la Aplicación a la información específica en cada caso.**
  - **(iv)prohibir la divulgación de información personal en el caso de los "amigos" de los usuarios que descargan una Aplicación.**

El 4 de abril de 2012[71], en una investigación adelantada contra Facebook, la OPC encontró que Facebook no había cumplido con su obligación de obtener el consentimiento por parte de los no usuarios para el tratamiento de la dirección de correo electrónico, con el fin de generar sugerencias de amigos.

El 24 de mayo de 2018[72], la OPC informó que el 20 de junio de 2013, **Facebook le había informado que esa compañía había sufrido un incidente de privacidad relativo a la divulgación de los datos de contactos de información suministrados por los usuarios de Facebook a través del proceso "Contact Importador"**.[73]

Con ocasión a la investigación adelantada, la OPC emitió una serie de recomendaciones a Facebook, entre las que se encuentran:

- Implementar mecanismos dirigidos a mejorar los sistemas de pruebas y de revisión de las interacciones entre las funcionalidades en Facebook, especialmente cuando dicha plataforma adhiere una nueva funcionalidad a un sistema existente.
- Desarrollar mecanismos para garantizar que los datos utilizados como parte de sus pruebas estén diseñados y / o seleccionados de manera más adecuada para reflejar la función que se está probando y que refleje mejor los datos contenidos en Facebook.
- Proporcionar a los usuarios información acerca de los procesos de "matching" entre las libretas de direcciones, con el fin de que estos estén adecuadamente informados sobre el uso de su información personal por parte de Facebook y, de esta manera, puedan entender razonablemente que ellos están consistiendo el uso de la información bajo este contexto.
- Suprimir la información de aquellas personas que Facebook no haya identificado como usuarios de la plataforma de red social, así como, abstenerse de usar, en el proceso de "matching" de las libretas de direcciones, la información de aquellos usuarios que no han sido identificados como usuarios. Lo anterior no es aplicable si Facebook obtiene el consentimiento de los no usuarios para el tratamiento de su información personal en el proceso de "matching" de las libretas de direcciones.
- Crear un sistema mediante el cual un usuario pueda acceder, bajo solicitud, a todos los datos relacionados a la información de contactos asociados a esa persona como resultado del proceso de "matching" de las libretas de direcciones, así como, solicitar la corrección cuando sea necesario.

El 5 de abril de 2018[74], la OPC anunció que esa oficina, en colaboración con la Oficina del Comisionado de la Información y Privacidad de la Columbia Británica (The Office of the Information and Privacy Commissioner for British Columbia), había iniciado **una investigación respecto de la**

---

[71] Cfr. The Office of the Privacy Commissioner of Canada (OPC), en: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2012/pipeda-2012-002/

[72] Cfr. The Office of the Privacy Commissioner of Canada (OPC), en https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2018/pipeda-2018-003/

[73] FB's Contact Importer tool is a feature that allows users to choose to upload and store their contacts as part of their accounts, and use such contacts to (i) invite other users to become their friends on Facebook, (ii) get friend suggestions and (iii) invite their contacts who are not users to join Facebook.

[74] Cfr. The Office of the Privacy Commissioner of Canada (OPC), en: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180320/ & https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_180405/

violación de la seguridad de los datos personales (o "data personal breach" o "privacy breach") en el caso de Facebook, Cambridge Analytica y "Aggregate IQ".

En el informe de junio del 2018 titulado "ADDRESSING DIGITAL PRIVACY VULNERABILITIES AND POTENTIAL THREATS TO CANADA'S DEMOCRATIC ELECTORAL PROCESS"[75], y realizado por el Comité de Acceso a la Información, Privacidad y Ética ("The Standing Committee on Access to Information, Privacy and Ethics") de la Cámara de Comunes del Parlamento de Canadá, en adelante "ETHI" por sus siglas en inglés relacionado con la violación de la seguridad de los datos personales en el caso Facebook, Cambridge Analytica y "Aggregate IQ"[76], se señala que **Facebook reconoció que**: (i) **no invirtió lo suficiente en la seguridad de la plataforma**; (ii) tampoco reconoció la gran responsabilidad que ellos tenían frente al uso de la plataforma por parte de los usuarios; y (iii) omitió centrar esfuerzos suficientes para prevenir el abuso de la misma[77].

El 1º de noviembre de 2018[78], el Comisionado de la OPC, el señor Daniel Therrien, presentó su **reporte sobre la violación de la seguridad de los datos personales en el caso Cambridge Analytica y Facebook** ante el "ETHI" de la Cámara de Comunes del Parlamento de Canadá.

Informó el Comisionado lo que sigue a continuación:

> *"(…) la investigación se está enfocando en el **acceso a la información personal proporcionada a terceros por Facebook, en particular, el suministro (o la acción de compartir) de información relacionada con los "amigos" con los desarrolladores de las Aplicaciones**. Este fue un grave problema en el 2008 y nosotros le informamos sobre esto a Facebook, hace casi una década.*
>
> *Desde mayo, los investigadores han emitido tres solicitudes extensas de información por separado y han recibido y revisado varios conjuntos de representaciones de Facebook en respuesta, y le pedimos a Facebook que detalle sus políticas y procedimientos a partir de 2013 en adelante.*
>
> *También hemos buscado información detallada sobre sus salvaguardas y el proceso interno de 'revisión de la aplicación', y el cumplimiento de los compromisos adquiridos con el OPC en 2009 y 2010."*[79]. (Negrillas fuera del texto original).

13.7. The Office of the Australian Information Commissioner (OAIC)

En mayo de 2012[80], la Oficina del Comisionado de Información de Australia (The Office of the Australian Information Commissioner), en adelante "OAIC" por sus siglas en inglés, emitió una serie de recomendaciones, bajo el concepto de "buenas prácticas" en relación con la actualización de las políticas de privacidad de Facebook, entre las que se encuentran:

- La política debería proporcionar un enlace a la guía sobre el perfil de línea de tiempo de Facebook o "Profile (Timeline) Review", incluido en el Centro de Ayuda de Facebook.
- Facebook debería: (i) informar a los usuarios sobre las Aplicaciones que han accedido o han recolectado su información personal; (ii) ser transparente acerca del tiempo que las Aplicaciones pueden acceder a la información del usuario; (iii) comunicar a los usuarios de los mecanismos

---

[75] Cfr. The Standing Committee on Access to Information, Privacy and Ethics (The House of Commons of Canada). "That, in light of the large data breach perpetrated by Cambridge Analytica and unreported by Facebook for several years, the Committee conduct a study of the privacy implications of platform monopolies and possible national and international regulatory and legislative remedies to assure the privacy of citizens' data and the integrity of democratic and electoral processes across the globe; including testimony from the Cambridge Analytica whistleblower, Christopher Wylie, the Privacy Commissioner of Canada, Daniel Therrien, as well as directors and executives of large platform companies such as Facebook, Amazon and Google". En: https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf

[76] Cfr. The Standing Committee on Access to Information, Privacy and Ethics (The House of Commons of Canada), en: https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-96/minutes

[77] Ibídem. "Kevin Chan, Global Director and Head of Public Policy for Facebook Canada, and Robert Sherman, Deputy Chief Privacy Officer for Facebook, appeared before the Committee on behalf of Facebook. While acknowledging that Facebook still did not have all the facts about Cambridge Analytica, Mr. Chan said that the situation was "a huge breach of trust" to Facebook users. The Facebook representatives recognized that the company committed the following mistakes: 1. Facebook had not invested enough in the security of its platform, and it takes responsibility for that; 2. Facebook did not do enough to prevent these powerful tools from being used for harm; 3. Facebook did not take a broad enough view of its responsibility; 4. "We recognize that, in the past, we have been too idealistic about the use of our technologies and we have not concentrated sufficiently on preventing abuse on our platform." 5. Facebook should have notified users affected by the Cambridge Analytica affair in 2016. 6. Regarding the way Facebook's platform worked before changes were made in 2014 to limit the information app developers could collect: "we don't think that's the right way for a platform to operate"; 7 Facebook was too slow to identify the threat of foreign interference through fake accounts and misinformation during the most recent presidential election in the United States." (Páginas 12 y 13).

[78] Cfr. The Office of the Privacy Commissioner of Canada (OPC), en: https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_20181101

[79] Traducción no oficial.

[80] Cfr. The Office of the Australian Information Commissioner (OAIC), en: https://www.oaic.gov.au/engage-with-us/submissions/changes-to-facebooks-data-use-policy

mediante los cuales pueden solicitar que las Aplicaciones eliminen su información personal; (iv) requerir a las Aplicaciones para que eliminen automáticamente los datos de los usuarios cuando estos remuevan las Aplicaciones, en lugar de solo hacerlo en respuesta a una solicitud directa del usuario, y (v) ser claro no solo sobre la información específica de localización que recolecta, sino cómo y cuándo dicha lo hace.

El 5 de abril de 2018[81], la OAIC anunció que esa entidad había abierto una investigación formal contra Facebook, con ocasión al anunció por parte de dicha compañía de que la información de más de 300,000 usuarios australianos podía haber sido adquirida y utilizada sin la autorización de ellos, en el caso Cambridge Analytica[82].

El 29 de septiembre de 2018[83], la OAIC anunció que Facebook, bajo "The Notifiable Data Breaches (NDB) scheme", le **informó sobre el incidente de seguridad que afectó a las cuentas de sus usuarios**[84].

13.8. The Office of the Privacy Commissioner of New Zealand (OPC)

El 28 de marzo de 2018[85], la Oficina del Comisionado de Privacidad de Nueva Zelanda (The Office of the Privacy Commissioner of New Zealand), en adelante "OPC", por sus siglas en inglés, encontró que Facebook había incumplido el "Privacy Act 1993".

Señaló la OPC lo siguiente:

(i) Facebook está sujeto al "Privacy Act 1993", en la medida en que ellos operan en Nueva Zelanda y proporcionan servicios a neozelandeses, independiente que el procesamiento de los datos personales se realice en el extranjero; y,

(ii) Facebook no cumplió con el "Privacy Act 1993", en la medida en que éste: se abstuvo de responder adecuadamente al requerimiento de información del titular, desconoció el ámbito de aplicación de "Privacy Act 1993", y se abstuvo de cooperar con la Autoridad de privacidad.

El 9 de abril de 2018[86], **la OPC informó que Facebook le había notificado que un total de 63,724 personas en Nueva Zelanda podrían haber sido impactadas por el uso de sus datos en el caso de Cambridge Analytica**.

En el reporte publicado el 19 de noviembre de 2018[87], la OPC informó que esa entidad **inició un proceso de llamamiento**[88] **a Facebook, después de que este se negará a cooperar con la investigación adelantada por el incidente de seguridad que afectó a la información personal de los usuarios de Nueva Zelanda**.

13.9. The Office of the Attorney General for the District of Columbia

El 19 de diciembre de 2018, el Fiscal General para el Distrito de Columbia (The Office of the Attorney General for the District of Columbia), en adelante la Oficina del Fiscal, anunció[89] que su oficina

---

[81] Cfr. The Office of the Australian Information Commissioner (OAIC), en: https://www.oaic.gov.au/media-and-speeches/statements/facebook-and-cambridge-analytica#investigation-into-facebook-opened

[82] **Cfr. El 13 de abril de 2018, la Comisión Nacional de Privacidad de las Filipinas ("The National Privacy Commission, NPC" anunció que, bajo la "Data Privacy Act 2012", esa autoridad inició una investigación contra Facebook por las fallas de la compañía en el escándalo de datos de Cambridge Analytica que afectó a los usuarios filipinos de Facebook**, en: https://www.privacy.gov.ph/2018/04/npc-opens-probe-on-facebook/

[83] Cfr. The Office of the Australian Information Commissioner (OAIC), en: https://www.oaic.gov.au/media-and-speeches/statements/security-of-facebook-accounts

[84] Cfr. **El 3 de octubre de 2018, la Oficina del Comisionado de Privacidad para los Datos Personales de Hong Kong (The Privacy Commissioner for Personal Data, Hong Kong) anunció que dicha entidad inició una verificación de cumplimiento respecto del incidente ocurrido a Facebook bajo la Personal Data (Privacy) Ordinance**, en: https://www.pcpd.org.hk/english/news_events/media_statements/press_20181003.html.

[85] Cfr. The Office of the Privacy Commissioner of New Zealand, en: https://www.privacy.org.nz/news-and-publications/statements-media-releases/privacy-commissioner-facebook-must-comply-with-nz-privacy-act/

[86] Cfr. The Office of the Privacy Commissioner of New Zealand, en: https://www.privacy.org.nz/news-and-publications/statements-media-releases/facebook-notification-of-new-zealanders-impacted-by-cambridge-analytica-breach/.

[87] Cfr. The Office of the Privacy Commissioner of New Zealand, en: https://www.privacy.org.nz/assets/Uploads/Privacy-Commissioner-Annual-Report-2018.pdf.

[88] Cfr. Cfr. The Office of the Privacy Commissioner of New Zealand. "Publicly naming organizations is one of the tools we use to incentivize compliance. We reserve this practice for specific situations, such as when an organization does not engage with our investigation process, a privacy breach was particularly serious or if we suspect the agency's conduct can also affect other people.", en: https://www.privacy.org.nz/assets/Uploads/Privacy-Commissioner-Annual-Report-2018.pdf.

[89] Cfr. The Office of the Attorney General for the District of Columbia, "Facebook Enforcement Action Press Call", en: https://oag.dc.gov/release/prepared-remarks-facebook-enforcement-action-press

había interpuesto una **demanda**[90] **contra Facebook, por las fallas en sus medidas de seguridad implementadas para proteger la información personal de sus usuarios**.

En su investigación, la Oficina del Fiscal descubrió lo siguiente:

- En el 2013, Facebook permitió a Aleksandr Kogan, un investigador afiliado a la Universidad de Cambridge, y su compañía, Global Science Research ("GSR"), operara una Aplicación en la plataforma de Facebook llamada "thisisyourdigitallife".
- Esta aplicación decía ser una "prueba de personalidad" y se ofreció para generar un perfil de personalidad **(perfilamiento)** a cambio de que los usuarios descargaran la Aplicación y autorizaran el acceso a la información de sus cuentas en Facebook.
- Los usuarios de Facebook autorizaron que la Aplicación recolectará los datos relacionados con su nombre, género, fecha de nacimiento, ciudad actual y "Like" o "me gusta".
- La Aplicación recolectó la información de los "amigos" de los usuarios que la descargaron en Facebook, aunque esas personas no habían otorgado el permiso a la Aplicación para compartir su información personal.
- Los reportes públicos indican que, en el año 2014, la compañía Global Science Research ("GSR") vendió la información personal recolectada a Cambridge Analytica, incluyendo los datos de millones de personas que nunca descargaron la Aplicación ni otorgaron su consentimiento para que esta consultara y usara su información personal (De hecho, sólo 862 residentes del Distrito de Columbia habían descargado "la prueba de personalidad", pero se encontró que los datos de más de 340.000 residentes en el Distrito de Columbia habían sido vendidos a Cambridge Analytica).
- Cambridge Analytica y sus clientes usaron la información personal para propósitos políticos en la campaña presidencial en el año 2016 de los Estados Unidos, en función de sus rasgos personales (o perfiles de personalidad).
- **A pesar de que Facebook conocía que la información personal de millones de sus usuarios fue recolectada y vendida en el año 2015, Facebook esperó más de dos años para comunicar el incidente ocurrido, tanto a sus usuarios como a las autoridades pertinentes**.

Por lo tanto, la oficina del Fiscal General concluyó lo siguiente[91]:

- Facebook no protegió la privacidad de sus usuarios y los engañó acerca de quién tenía acceso a sus datos personales y cómo estos fueron usados.
- Facebook pone a los usuarios en riesgo de manipulación al permitir que compañías, como Cambridge Analytica, recopilen datos personales sin el permiso de los usuarios[92].
- **Facebook no cumplió con su compromiso de contar con las medidas necesarias para proteger los datos de los usuarios**.

---

[90] Cfr. The Office of the Attorney General for the District of Columbia, copia de demanda en: http://oag.dc.gov/sites/default/files/2018-12/Facebook-Complaint.pdf

[91] Cfr. The Office of the Attorney General for the District of Columbia, "Facebook Enforcement Action Press Call", en: https://oag.dc.gov/release/ag-racine-sues-facebook-failing-protect-millions. Cita el comunicado de prensa: "An investigation by OAG found that this abuse was among the many examples of Facebook's failure to protect consumers' data adequately. The investigation found that Facebook violated the District's Consumer Protection Procedures Act (CPPA), which prohibits unfair and deceptive trade practices. Among the ways that Facebook harmed consumers, the complaint alleges, are: (i) **Misleading users about the security of their data**: Facebook represented to users that it would protect the privacy of their personal information, and that it required applications and third-party developers to respect consumers' privacy. However, Facebook allowed Kogan to collect and sell the data of users who had not downloaded or used Kogan's app; (ii) **Failing to properly monitor third-party apps' use of data:** Although Facebook was aware as early as 2014 that Kogan wanted to download the personal information not only of his app's users, but also of his users' friends, Facebook failed to monitor or audit the app to see if it was abiding by Facebook's policies for third-party applications and user data; (iii) **Making it difficult for users to control data settings for apps:** Facebook maintained confusing and ambiguous privacy and applications settings that made it difficult for consumers to control how their data was shared. Instead of allowing users to control access to their information on third-party apps directly from its main privacy settings page, Facebook required users to go to a different part of its platform for third-party app privacy settings. This made it harder for consumers to realize that apps could be harvesting their data; (iv) **Failing to disclose the Cambridge Analytica breach to consumers for more than two years:** Facebook first became aware in 2015 that Cambridge Analytica had obtained millions of users' data. The company conducted a cursory investigation and confirmed that the data had been improperly harvested from users and then sold to Cambridge Analytica. However, Facebook did not inform users affected by the breach until 2018; (v) **Failing to ensure users' improperly obtained data was deleted:** Even after it confirmed its users' data had been improperly harvested, Facebook took Cambridge Analytica at its word that the company had deleted the data. They did this even though Facebook staffers were embedded with the Trump campaign and other campaigns, working alongside Cambridge Analytica staff to use the data to target voters; (vi) **Failing to inform consumers that some companies could override data privacy settings; (vii)** Facebook also failed to inform consumers that it granted certain companies, many of whom were mobile device makers, special permissions that enabled those companies to access consumer data and override consumer privacy settings. (Traducción no official).

[92] Cfr. Ibidem. Subraya el comunicado de prensa: "Facebook failed to protect the privacy of its users and deceived them about who had access to their data and how it was used," said AG Racine. "Facebook put users at risk of manipulation by allowing companies like Cambridge Analytica and other third-party applications to collect personal data without users' permission. Today's lawsuit is about making Facebook live up to its promise to protect its users' privacy." (Traducción no official).

- La política de "Términos de servicio" de Facebook señala que dicha empresa requiere que los desarrolladores de Aplicaciones respeten la privacidad de los usuarios, y solo les permite acceder a la información del usuario que descarga la Aplicación en Facebook. Sin embargo, durante el escándalo de Cambridge Analytica, la oficina del Fiscal encontró que Facebook no cumplió sus propias políticas corporativas dirigidas a monitorear la forma en que las Aplicaciones de terceros estaban usando los datos recopilados por ellas, lo que llevó, en el caso de Cambridge Analytica, a que esta comercializará la información personal recolectada, en violación expresa de la política propia de Facebook.
- La Aplicación "thisisyourdigitallife" contenía términos que contradecían directamente la política de Facebook, indicando expresamente que los datos recopilados podrían utilizarse con fines comerciales. Sin embargo, Facebook no adoptó ninguna medida contra la Aplicación y, en cambio, le permitió vender los datos de los usuarios de Facebook sin, según el comunicado de prensa de la oficina del Fiscal, supervisión.
- Aunque Facebook conocía que el señor Aleksandr Kogan quería descargar los datos personales no solo de los usuarios de la Aplicación sino de los amigos de los usuarios, **Facebook falló en monitorear o auditar la Aplicación para determinar si esta estaba cumplimiento con sus políticas dirigidas a los desarrolladores de Aplicaciones y usuarios de Facebook**.
- Una vez Facebook tuvo conocimiento que los datos personales de sus usuarios se estaban usando de una manera contraria con sus políticas, Facebook no se aseguró que Cambridge Analytica eliminara definitivamente la información
- Las configuraciones de privacidad y de las Aplicaciones no permiten de una manera clara a los usuarios tener un control de cómo sus datos se comparten. En la investigación, se encontró que en lugar de permitir a los usuarios controlar el acceso a su información en Aplicaciones de terceros directamente desde su página principal de configuración de privacidad, Facebook requirió que los usuarios fueran a una parte diferente de su plataforma para la configuración de privacidad de la Aplicación de terceros. **Esto hizo que a los consumidores les resultara más difícil darse cuenta de que las aplicaciones podrían estar recolectando sus datos**.

La oficina del Fiscal busca con la citada demanda que Facebook:

(i) **asuma la responsabilidad por las fallas de seguridad y la exposición de la información personal de sus usuarios**; y,

(ii) **desarrolle nuevos protocolos que protejan, de manera efectiva, los datos de sus usuarios para asegurar que un evento como el sucedido no ocurra nuevamente**.

DÉCIMO CUARTO: Que con base en el mencionado reporte publicado por el diario británico "The Guardian", en colaboración con "The New York Times" y "The Observer", esta Dirección decidió iniciar una indagación preliminar contra Facebook.

14.3.1. El día 26 de marzo de 2018, la Dirección de Investigación realizó una visita de inspección en las instalaciones de Facebook Colombia SAS, con el fin de verificar el cumplimiento de la normatividad en protección de datos personales[93].

En la diligencia, el representante legal suplente, "Country Manager", precisó lo siguiente: (i) actualmente no se cuenta con un departamento administrativo y todos los servicios legales están tercerizados y solo se hacen reportes comerciales a la "casa matriz"; y, (ii) respecto de la seguridad de los datos personales afectados en el incidente que involucra a Facebook y Cambridge Analytica, dichos temas están centralizados en Estados Unidos. Lo único que se realizó desde Facebook Colombia fue remitir los comunicados oficiales expedidos por la compañía a los clientes corporativos.

En todo caso, esta Dirección le solicitó a Facebook Colombia SAS que respondiera lo siguiente[94]: (i) si dentro de la información de usuarios utilizada por "Cambridge Analytica" se encuentran cuentas de usuarios en Colombia; y, (ii) en caso afirmativo, cuántos usuarios fueron afectados y si se le informó lo sucedido.

Adicionalmente, se le solicitó comunicar a los resultados de la investigación interna realizada por la compañía anunciada en su comunicación del 24 de marzo de 2018.

[redacted]

[94] Radicado No. 18-105923-1

14.3.2. Mediante escrito radicado con el número 18-105923-4 el 11 de abril de 2018[95], Facebook Colombia SAS informó que:

[redacted]

14.3.3. Mediante comunicación radicada con el número 18-105923-5 el 11 de abril de 2018[96], Facebook Ireland Limited resumió la falla de seguridad ocurrida a Facebook en el caso Cambridge Analytica:

[redacted]

14.3.4. Mediante comunicado allegado el 1º de junio de 2018[97], con radicado No. 18-105923,-17 Facebook Ireland Limited informó lo siguiente:

[95] Folio 38.
[96] Folios 43 – 214.
[97] Folios 269 -451.

[redacted]

14.3.5. Mediante comunicado allegado el 13 de junio de 2018[98], Facebook Ireland Limited reitera lo siguiente:

[redacted]

DÉCIMO QUINTO: Que de todo lo anterior se concluye, entre otras, lo siguiente:

a) Facebook recolecta y trata datos personales de miles de millones de personas de todo el mundo y de más de 31 millones de colombianos.
b) Facebook usa y circula los datos de manera global y transfronteriza.
c) Facebook anuncia en su página web que ha desarrollado *políticas herramientas y recursos para proteger los datos personales*[99].

[98] Folios 452-455.
[99] Cfr. https://www.facebook.com/safety . Última consulta: 24 de enero de 2019

d) No obstante lo anterior, los hechos, las investigaciones y las actuaciones de autoridades de protección de datos de ocho (8) países del mundo *(Irlanda, Estados Unidos, Gran Bretaña, Francia, Países Bajos, Canadá, Australia y Nueva Zelanda)* y las acciones judiciales iniciadas por el Fiscal General del Distrito de Columbia (Estados Unidos), permiten establecer que Facebook:

(i) No ha adoptado las medidas de seguridad suficientes y efectivas para impedir que los datos de sus usuarios fueran accedidos y compartidos por un tercero en contravía de la normatividad en protección de datos personales en diferentes países y sus políticas de privacidad y, en algunos casos, sin contar el consentimiento de los titulares (en el caso de los "amigos" de los usuarios que descargan una Aplicación).

(ii) Ha reconocido vulnerabilidades en su plataforma que permitió a terceros hurtar "tokens" de acceso a Facebook, que luego podrían ser empleadas para tomar el control de cuentas de usuarios.

(iii) Ha admitido que por fallas en el "Photo API" se generó que terceros desarrolladores de Aplicaciones (1.500 Aplicaciones construidas por 876 desarrolladores), accedieran a gran cantidad de fotografías de alrededor de 5.6 millones de usuarios, por el periodo de 12 días entre el 13 al 25 de septiembre de 2018).

En suma, las medidas de seguridad de Facebook no son suficientes ni adecuadas para garantizar la seguridad de los datos de millones de personas. Lo anterior es muy grave porque la seguridad es un elemento esencial para realizar un debido tratamiento de esa información y proteger los derechos humanos.

DÉCIMO SEXTO: Que la seguridad de la información es una condición crucial del tratamiento de datos personales. Una vez recolectados deben ser objeto de medidas de diversa índole para evitar situaciones indeseadas que pueden afectar los derechos de los titulares y de los mismos Responsables y Encargados del tratamiento de los datos. El acceso, la consulta y el uso no autorizado o fraudulento, así como la manipulación y pérdida de la información son los principales riesgos que se quieren mitigar a través de medidas de seguridad de naturaleza humana, física, administrativa o técnica.

La seguridad ha sido una preocupación del legislador y la Corte Constitucional. Esta última concluyó que "*debe reiterarse que el manejo de información no pública debe hacerse bajo todas las medidas de seguridad necesarias para garantizar que terceros no autorizados puedan acceder a ella. De lo contrario, tanto el responsable como el Encargado del Tratamiento serán los responsables de los perjuicios causados al Titular*"[100].

La seguridad de los datos personales no se limita situaciones de infiltración o burla de las medidas de seguridad que ha implementado un Responsable o Encargado del Tratamiento. La 1581 de 2012 va más allá porque exige lo siguiente:

> *"ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES. En el desarrollo, interpretación y* ***aplicación*** *de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios (…)*
>
> *g) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros* ***evitando*** *su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;*
>
> *ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: (…)*
>
> *d) Conservar la información bajo las condiciones de seguridad necesarias para* ***impedir*** *su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;"*
>
> *"ARTÍCULO 18. DEBERES DE LOS ENCARGADOS DEL TRATAMIENTO. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: (…)*

[100] Cfr. Corte Constitucional, Sentencia C-748 de 2011.

*b) Conservar la información bajo las condiciones de seguridad necesarias para **impedir** su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;"*

Nótese que la redacción del principio de seguridad tiene un criterio eminentemente preventivo, lo cual obliga a los responsables o encargados a adoptar las medidas necesarias para evitar posibles afectaciones a la seguridad de los datos.

Este carácter preventivo obliga a los Responsable y Encargados a identificar sus vulnerabilidades con el objetivo de implementar o reforzar sus medidas de seguridad.
Es preciso aclarar que la implementación de medidas de seguridad por parte de los Responsables y Encargados del tratamiento no está supeditada o condicionada a que exista un daño o perjuicio de los derechos o intereses que se buscan proteger con la Ley 1581 de 2012. El solo hecho de tratar datos personales es suficiente. Una interpretación en sentido contrario, no solo iría en contra de la naturaleza preventiva que se deriva expresamente de los textos legales citados, sino que privaría a los colombianos de la capacidad de exigir a los Responsables y Encargados que aseguren un nivel adecuado de protección en relación con sus datos.

DÉCIMO SÉPTIMO. Que la regulación colombiana exige a Facebook responsabilidad demostrada respecto de las medidas de seguridad para realizar tratamiento de datos personales. En efecto, los artículos 26 y 27 del Decreto 1377 de 2013 (*incorporados en el decreto 1074 de 2015*) dicen lo siguiente:

"*Artículo 26. Demostración. 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 y este decreto, en una manera que sea proporcional a lo siguiente:*

1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.

2. La naturaleza de los datos personales objeto del tratamiento.

3. El tipo de Tratamiento.

4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares. (...)

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas" (Subrayamos)

Artículo 27. Políticas internas efectivas. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar:

1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto.

2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.

3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento." (Subrayado fuera del texto original).

Sobre la responsabilidad demostrada nos remitimos a lo señalado por la Superintendencia de Industria y Comercio mediante la Resolución 83882 del 15 de noviembre de 2018:

La regulación colombiana le impone al Responsable o al Encargado del tratamiento la responsabilidad de garantizar el cumplimiento de la ley 1581 de 2012, la cual no puede ser simbólica ni formal, sino real y demostrable. Téngase presente que según nuestra jurisprudencia "*existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante*"[101].

Adicionalmente, los Responsables o Encargados del tratamiento no son dueños de los datos personales que reposan en sus bases de datos o archivos. En efecto, ellos son meros tenedores que están en el deber de administrar de manera correcta, apropiada y acertada la información de las personas porque su negligencia o dolo en esta materia afecta los derechos humanos de los titulares de los datos.

En virtud de lo anterior, el capítulo III del Decreto 1377 del 27 de junio de *2013 -incorporado en el Decreto 1074 de 2015-* reglamenta algunos aspectos relacionados con el principio de responsabilidad demostrada. El artículo 26 *-titulado DEMOSTRACIÓN-* establece 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*" y dicho decreto.

Nótese como le corresponde al Responsable o al Encargado probar que ha puesto en marcha medidas adecuadas, útiles y eficaces para cumplir la regulación. Lo anterior significa que un administrador no puede utilizar cualquier tipo de política o herramienta para dicho efecto sino sólo aquellas que sirvan para que los postulados legales no sean meras elucubraciones teóricas sino realidades verificables.

El artículo 27 *-denominado POLÍTICAS INTERNAS EFECTIVAS-*, por su parte, exige que los Responsables implementen medidas efectivas y apropiadas que garanticen, entre otras, lo siguiente: "*(…) 1. (…) la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto*".

Con el propósito de dar orientaciones sobre la materia, la Superintendencia de Industria y Comercio expidió el 28 de mayo de 2015 la *"Guía para implementación del principio de responsabilidad demostrada (accountability)"*[102]. El término "*accountability*" proviene del mundo anglosajón[103] y a pesar de las diferentes acepciones que puedan darse sobre el significado del mismo, se ha entendido que en la arena de la protección de datos dicha expresión se refiere no sólo al modo como una organización debe cumplir en la práctica las regulaciones sobre el tema, sino a la manera como debe demostrar que lo hecho es útil, pertinente y eficiente.

En línea con lo anterior, la precitada guía recomienda lo siguiente a los obligados a cumplir la Ley 1581 de 2012:

(1) Diseñar y poner en marcha un programa integral de gestión de datos (en adelante PIGDP), lo cual exige compromisos y acciones concretas de los directivos de la organización, así como la implementación de controles de diversa naturaleza que se enuncian en el texto de la guía;
(2) Desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP, y
(3) Demostrar el debido cumplimiento de la regulación sobre tratamiento de datos personales.

El principio de responsabilidad demostrada –*accountability*- demanda implementar acciones de diversa naturaleza[104] para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El mismo exige que los Responsables y Encargados del tratamiento implementen medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia. Dichas medidas deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los datos personales.

El principio de responsabilidad demanda menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. Éste exige

[101] Cfr. Corte Constitucional, sentencia T-227 de 2003.
[102] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf
[103] Cfr. Grupo de trabajo de protección de datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 8.
[104] Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humanas y de gestión que involucran procesos y procedimientos.

implementar acciones concretas por parte de las organizaciones para garantizar el debido tratamiento de los datos personales. El éxito del mismo dependerá del compromiso real de todos los miembros de una organización pero, especialmente, de los directivos de las organizaciones ya que sin su apoyo franco y decidido todo esfuerzo será insuficiente para diseñar, implementar, revisar, actualizar y evaluar los programas de gestión de datos.

Adicionalmente, el reto de las organizaciones frente al principio de responsabilidad demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas porque exige que se demuestre el cumplimiento real y efectivo en la práctica cuando realizan sus funciones. En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que "*la autorregulación sólo redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que* ***no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales***"[105] (Negrillas fuera del texto original).

El principio de responsabilidad demostrada busca que los mandatos constitucionales y legales sobre tratamiento de datos personales sean una realidad verificable y redunden en beneficio de la protección de los derechos de las personas. Por eso, es crucial que los administradores de las organizaciones sean proactivos respecto del tratamiento de la información de manera que por iniciativa propia adopten medidas estratégicas capaces de garantizar, entre otras, la seguridad en el tratamiento de la información.

Aunque no es este el espacio para explicar cada uno de los anteriores aspectos mencionados en la guía[106], ponemos de presente que la identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales de lo que implica el principio de responsabilidad demostrada (accountability). En la mencionada guía se considera fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un "*sistema de administración de riesgos asociados al tratamiento de datos personales*"[107] que les permita "*identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales*"[108].

La debida administración de datos implica, entre otras cosas, garantizar el principio de seguridad. En otras palabras, el tratamiento de datos que desconozca ese principio no es consistente con la Constitución ni la ley. Ese tipo de administración no es admisible a la luz de la regulación colombiana y no puede convertirse en una práctica empresarial ni es tolerable por las autoridades que según el artículo 2 de la Constitución *"están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades (…)."*

Dada su relevancia con el tema, nos permitimos recordar algunos mandatos constitucionales relacionados con el cumplimiento de la ley, el respeto de los derechos humanos y las responsabilidades que implica el ejercicio de las libertades y los derechos. Todos ellos tienen plena aplicabilidad en el tratamiento de datos personales.

Primero: *"el ejercicio de los derechos y libertades reconocidos en esta Constitución implica responsabilidades"* [109].

Segundo: la realización de la actividad empresarial "*implica obligaciones*" [110].

Tercero: "*toda persona está obligada a cumplir la Constitución y las leyes*" [111].

---

[105] Cfr. Red Iberoamericana de Protección de Datos. Grupo de trabajo temporal sobre autorregulación y protección de datos personales. Mayo de 5 de 2006. En aquel entonces, la RIPD expidió un documento sobre autorregulación y protección de datos personales que guarda cercana relación con "accountability" en la medida que la materialización del mismo depende, en gran parte, de lo que internamente realicen las organizaciones y definan en sus políticas o regulaciones internas.
[106] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf
[107] Cfr. Superintendencia de Industria y Comercio (2015) "*Guía para implementación del principio de responsabilidad demostrada (accountability)*". Págs 16-18
[108] Ibidem. Pág. 16
[109] Cfr. Artículo 95 de la Constitución Política de Colombia
[110] Cfr. Artículo 333 de la Constitución Política de Colombia
[111] Cfr. Artículo 95 de la Constitución Política de Colombia

Cuarto: "*es deber de los nacionales y de los extranjeros en Colombia acatar la Constitución y las leyes, y respetar y obedecer a las autoridades*"[112].

Quinto: "***En la recolección, tratamiento y circulación de datos*" se debe respetar "*la libertad y demás garantías consagradas en la Constitución***" [113]. (Se destaca)

DÉCIMO OCTAVO: Que, se reitera, Facebook es la red social digital con mayor número de usuarios en el mundo y en la República de Colombia. En efecto, Facebook tiene aproximadamente 2.410[114] millones de usuarios en todo el mundo de los casi 4.130[115] millones de internautas. En otras palabras, Facebook trata datos personales de no menos del 58% de las personas que tienen acceso a internet.

En cuanto a Colombia, la cifra de usuarios de Facebook oscila entre 20[116] y 31[117] millones de personas. Si se toma este último dato y se tiene en cuenta la población colombiana (45.5 millones) según DANE[118], se puede concluir que Facebook trata los datos personales del 68% de los colombianos.

Facebook tiene la enorme responsabilidad de garantizar la seguridad de la información de todos sus usuarios, lo cual lo obliga a ser extremadamente diligente en esta labor y a no ahorrar esfuerzos para responder por la seguridad de los datos de miles de millones de personas.

Es innegable el impacto masivo que pueden generar las medidas de seguridad Facebook sobre gran parte de la población colombiana. Por eso, esta Dirección considera necesario impartir a Facebook directrices con **CARÁCTER PREVENTIVO** para evitar que sucedan incidentes de seguridad como los relacionados en esta resolución que puedan afectar a personas residentes o domiciliadas en la República de Colombia.

DÉCIMO NOVENO. Que teniendo en cuenta todo lo anterior, y en especial lo que ordena el principio y el deber de seguridad, así como lo que implica el cumplimiento del principio de responsabilidad demostrada (*accountability*), este Despacho considera necesario impartir, con carácter PREVENTIVO, las órdenes que se indicarán en la parte resolutiva del presente acto administrativo.

VIGÉSIMO: Que para continuar garantizando el derecho de defensa y contradicción dentro de la presente actuación, el expediente queda a disposición de Facebook Inc., Facebook Colombia SAS y Facebook Ireland Limited en las instalaciones de esta Superintendencia.

En mérito de lo expuesto, este Despacho

RESUELVE

ARTÍCULO PRIMERO: Ordenar a Facebook Inc., Facebook Colombia SAS y Facebook Ireland Limited (en adelante Facebook) que procedan a realizar o implementar lo que sigue a continuación respecto del tratamiento de los datos personales de las personas naturales residentes o domiciliadas en la República de Colombia y que son usuarias de los servicios de dichas empresas (Facebook), o sobre las cuales Facebook trata, directa o indirectamente, la citada información:

1. Facebook deberá adoptar medidas nuevas, necesarias, apropiadas, útiles, eficaces y demostrables para cumplir el cien por ciento (100%) de lo que exige el principio y el deber de seguridad en la regulación colombiana, a saber:

a) Garantizar la seguridad de los datos personales, evitando lo siguiente respecto de los mismos:
(i) Acceso no autorizado o fraudulento
(ii) Uso no autorizado o fraudulento

---

[112] Cfr. Artículo 4 de la Constitución Política de Colombia
[113] Cfr. Artículo 15 de la Constitución Política de Colombia
[114] Cfr. http://www.internetlivestats.com/. Última consulta: 23 de enero de 2019
[115] Cfr. http://www.internetlivestats.com/. Última consulta: 23 de enero de 2019
[116] Cfr. Facebook supera los 20 millones de usuarios en Colombia. Publicado en: http://colombia-inn.com.co/facebook-supera-los-20-millones-de-usuarios-en-colombia/ . Última consulta: 23 de enero de 2019
[117] Cfr. Latamclick (2018) Estadísticas de Facebook (América Latina) 2018 con imágenes to Share. Publicado en: https://www.latamclick.com/estadisticas-de-facebook-america-latina-2018/. Última consulta: 23 de enero de 2019
[118] Cfr. DANE. Censos y demografía. Información sobre el censo de población de 2018. Datos preliminares a noviembre de 2018. Publicado en: https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/censo-nacional-de-poblacion-y-vivienda-2018/cuantos-somos. Última consulta: 23 de enero de 2018

(iii) Consulta no autorizada o fraudulenta
(iv) Adulteración no autorizada o fraudulenta
(v) Pérdida no autorizada o fraudulenta

2. Facebook deberá mejorar o robustecer las medidas de seguridad que ha implementado a la fecha de expedición de la presente resolución para cumplir el cien por ciento (100%) de lo que exige el principio y el deber de seguridad en la regulación colombiana, a saber:

a) Garantizar la seguridad de los datos personales, evitando lo siguiente respecto de los mismos:
(i) Acceso no autorizado o fraudulento
(ii) Uso no autorizado o fraudulento
(iii) Consulta no autorizada o fraudulenta
(iv) Adulteración no autorizada o fraudulenta
(v) Pérdida no autorizada o fraudulenta

3. Facebook deberá desarrollar, implementar y mantener un programa integral de seguridad de la información, que garantice la seguridad, confidencialidad e integridad de los datos personales, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El programa deberá constar por escrito, ser sujeto a pruebas periódicas para evaluar su efectividad, y tener en cuenta, como mínimo, lo siguiente:

(i) los principios rectores establecidos en la Ley 1581 de 2012 y los deberes que de ellos se derivan;
(ii) el tamaño y la complejidad de las operaciones de Facebook;
(iii) la naturaleza y el ámbito de las actividades de Facebook;
(iv) la categoría y cantidad de titulares;
(v) la naturaleza de los datos personales;
(vi) el tipo de tratamiento de los datos personales;
(vii) el alcance, contexto o fines del tratamiento;
(viii) el uso de los datos personales por terceros, entre ellos, aliados comerciales, empresas asociadas y desarrolladores de Aplicaciones;
(ix) el uso innovador o aplicación de nuevas soluciones tecnológicas; y,
(x) los riesgos para los derechos y libertades de las personas.

4. Facebook deberá desarrollar, implementar y mantener evaluaciones de impacto en la protección datos personales (o evaluaciones de impacto en privacidad), "DPIAs" o "PIAs" por sus nombres en inglés, que evalúen los riesgos inherentes al tratamiento de dicha información respecto del uso de la plataforma web o la Aplicación móvil complementaria de Facebook, sus productos, o cualquier otro medio a través del cual Facebook recolecte, use o comparta datos personales. Las evaluaciones deberán constar por escrito y estar disponibles en caso que las requiera esta Dirección. Las mismas, deberán tener en cuenta, como mínimo, lo siguiente:

(i) los principios rectores establecidos en la Ley 1581 de 2012 y los deberes que de ellos se derivan;
(ii) el tamaño y la complejidad de las operaciones de Facebook;
(iii) la naturaleza y el ámbito de las actividades de Facebook;
(iv) la categoría y cantidad de titulares;
(v) la naturaleza de los datos personales;
(vi) el tipo de tratamiento de los datos personales
(vii) el alcance, contexto o fines del tratamiento;
(viii) el uso de los datos personales de los usuarios por terceros, entre ellos, aliados comerciales, empresas asociadas y desarrolladores de Aplicaciones;
(ix) el uso innovador o aplicación de nuevas soluciones tecnológicas; y,
(x) los riesgos para los derechos y libertades de las personas.

5. Facebook deberá desarrollar, implementar y mantener un programa de gestión y manejo de violaciones de seguridad en datos personales, que contemple procedimientos para informar sin dilación indebida a esta Autoridad de protección de datos y a los titulares de los mismos cuando se presenten incidentes que afecten la confidencialidad, integridad y disponibilidad de los datos.

6. Facebook deberá desarrollar, implementar y mantener las medidas necesarias para impedir el acceso por parte de terceros, incluido, pero no limitado a, aliados comerciales, empresas asociadas o desarrolladores de Aplicaciones, a: (i) los datos personales de los usuarios y la de sus contactos o "amigos", sin su consentimiento, o (ii) información que no sea necesaria para el servicio o producto adquirido por los usuarios, para el funcionamiento de la Aplicación.

7. Facebook deberá modificar sus configuraciones de privacidad, de tal manera que estas le permitan a los usuarios: (i) controlar, de forma sencilla, fácil y rápida, el tipo de información que desean compartir con las Aplicaciones; (ii) conocer las Aplicaciones con las cuales se está compartiendo su información; (iii) acceder a las políticas de protección de datos (o privacidad) de las Aplicaciones y poder desactivar estas últimas para que no accedan a su información personal.

8. Facebook deberá desarrollar, implementar y mantener medidas que garanticen de manera efectiva la devolución o supresión de los datos personales, una vez finalizado el tratamiento de los mismos por parte de terceros tales como aliados comerciales, empresas asociadas o desarrolladores de aplicaciones.

9. Facebook deberá ajustar los contratos o acuerdos comerciales que suscriba con terceros, incluido, pero no limitado a, aliados comerciales, empresas asociadas o desarrolladores de Aplicaciones, para que el tratamiento de los datos personales de los usuarios cumpla con lo establecido en la Ley 1581 de 2012.

10. Facebook deberá desarrollar, implementar y mantener las acciones correctivas necesarias frente a aquellos terceros, incluido, pero no limitado a, aliados comerciales, empresas asociadas o desarrolladores de Aplicaciones, que incumplan la Ley 1581 de 2012, o las políticas de tratamiento de información personal (o políticas de privacidad) o las políticas corporativas de Facebook.

11. Facebook deberá efectuar una auditoría independiente, dentro de los cuatro (4) meses siguientes a la ejecutoria del presente acto administrativo, y cada año después de dicha fecha durante los próximos cinco (5) años, que certifique que cuenta con las medidas técnicas, humanas, administrativas, contractuales y de cualquier otra naturaleza que sean necesarias para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

ARTÍCULO SEGUNDO: Facebook Inc., Facebook Colombia SAS y Facebook Ireland Limited deberán obrar de la siguiente manera para efectos de lo que establece el artículo 26 del decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015) respecto de la demostración o evidencia ante esta Dirección del cumplimiento de las medidas, instrucciones, requerimientos u órdenes emitidas mediante esta resolución:

Facebook Inc., Facebook Colombia SAS y Facebook Ireland Limited deberán cumplir lo ordenado en esta resolución dentro de cuatro (4) meses siguientes a la ejecutoria del presente acto administrativo. Para demostrar el cumplimiento deberán remitir, al finalizar dicho término, una certificación emitida por una entidad o empresa independiente, imparcial, profesional, especializada y autorizada que acredite que se han implementado las medidas ordenadas por esta Dirección y que las mismas están operando con suficiente efectividad para proporcionar el grado de seguridad que exige el principio y el deber de seguridad de la ley 1581 de 2012 respecto de los datos personales.

La entidad o empresa que emita el certificado será seleccionada por Facebook, pero debe ser un tercero cuya gestión esté libre de todo conflicto de interés que le reste independencia y ajena a cualquier tipo de subordinación respecto de Facebook.

PARÁGRAFO: La entidad o empresa certificadora deberá ser autorizada por la autoridad competente del país de su domicilio, sólo en el caso que la regulación del mismo exija dicha autorización para poder emitir certificaciones. Si en dicho país no se exige lo anterior, bastará con que la misma sea independiente, imparcial, profesional y especializada en temas de seguridad de la información.

ARTÍCULO TERCERO: Ordenar a Facebook Colombia SAS que preste su colaboración para que Facebook Inc. y Facebook Ireland Limited cumplan las instrucciones y órdenes impartidas por esta Superintendencia en esta resolución.

ARTÍCULO CUARTO: Notificar el contenido de la presente resolución a Facebook Inc. Facebook Colombia SAS y Facebook Ireland Limited, informándoles que contra el presente acto administrativo procede recurso de reposición ante el Director de Investigación de Protección de Datos Personales y de apelación ante el Superintendente Delegado para la Protección de Datos Personales, dentro de los diez (10) días siguientes a la diligencia de notificación.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., 24 ENE. 2019

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUÑOZ

AMCC/CESM

NOTIFICACIÓN:

Investigada:	**FACEBOOK IRELAND LIMITED**
Identificación:	Sin identificar
Dirección:	4 Grand Canal Square, Grand Canal Harbour
Ciudad:	Dublin 2.
País:	Irlanda
Representante:	GARETH LAMBE
Identificación:	Sin identificación
Investigada:	**FACEBOOK INC**
Identificación:	Sin identificar
Dirección:	1601 Willow Road
Ciudad:	Menlo Park 94025 (Estado de California)
País:	Estados Unidos
Representante:	NAZNEEN DINYAR MEHTA
Identificación:	No. 2921781
Sociedad:	**FACEBOOK COLOMBIA S.A.S**
Identificación:	Nit. 900.710.525
Representante Legal:	CREHAN SHANE HUGH
Identificación:	P.P. PT9763807
Dirección:	Calle 90 No. 11-13 piso 5
Ciudad:	Bogotá, D.C.
Correo electrónico:	office.bogota@bakermckenzie.com