REPÚBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 12192 DE 2020

(01 de Abril de 2020)

Radicación 18-233402

VERSIÓN PÚBLICA

El Superintendente Delegado para la 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 por el numeral 7 del artículo 16 del Decreto 4886 de 2011, y

CONSIDERANDO

PRIMERO. Que mediante Resolución No. 1321 de 24 de enero de 2019[1], la Dirección de Investigación de Protección de Datos Personales resolvió impartir las siguientes órdenes a las sociedades Facebook Inc., Facebook Colombia S.A.S. y Facebook Ireland Limited:

> ***"ARTÍCULO PRIMERO:*** *Ordenar a Facebook Inc., Facebook Colombia S.A.S. y Facebook Ireland Limited (en adelante Facebook) que procedan a realizar o implementar lo que sigue a continuación respecto del tratamiento* [sic] *de los datos* [sic] *personales de las personas naturales residentes o domiciliadas en la República de Colombia y que son usuarios 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* [sic] *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* [sic] *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*
>
> ***2.*** *Facebook deberá mejorar o robustecer las medidas que ha implementado a la fecha de expedición de la presente resolución para cumplir el cien* [sic] *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* [sic] *personales, evitando lo siguiente respecto de los mismos:*
> *(i) Acceso no autorizado o fraudulento*

[1] Folios 456 a 470

(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 integralidad de los datos* [sic] *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 libertadores de las personas.

4. *Facebook deberá desarrollar, implementar y mantener evaluaciones de impacto en la protección de datos* [sic] *personales (o evaluaciones de impacto en privacidad), "DPIAs" o "PIAs" por sus nombres en inglés, que evalúen los riesgos inherentes al tratamiento* [sic] *de dicha información respecto del uso de la plataforma web o la Aplicación* [sic] *móvil complementaria de Facebook, sus productos, o cualquier otro medio a través del cual Facebook recolecte, use o comparta datos* [sic] *personales. Las evaluaciones deberán constar por escrito y estar disponibles en caso* [sic] *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 los 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* [sic] *personales, que contemple procedimientos para informar sin dilación indebida a esta Autoridad de protección de datos* [sic] *y a los titulares* [sic] *de los mismos cuando se presenten incidentes que afecten la confidencialidad, integridad y disponibilidad de los datos* [sic].

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* [sic]*, a: (i) los datos* [sic] *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* [sic]*.*

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* [sic]*; (ii) conocer las Aplicaciones* [sic] *con las cuales se está compartiendo su información; (iii) acceder a las políticas de protección de datos* [sic] *(o privacidad) de las Aplicaciones* [sic] *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* [sic] *personales, una vez finalizado el tratamiento* [sic] *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* [sic]*, para que el tratamiento* [sic] *de los datos* [sic] *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* [sic]*, que incumplan la Ley 1581 de 2012, o las políticas de tratamiento* [sic] *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* [sic] *personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*

ARTÍCULO SEGUNDO: *Facebook Inc., Facebook Colombia S.A.S. y Facebook Ireland Limited deberán obrar de la siguiente manera para efectos de lo que establece el artículo 26 del decreto* [sic] *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 S.A.S. 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 deberá 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 [sic] *personales.*

La entidad o empresa que emita el certificado será seleccionada por Facebook, pero debe ser un tercero cuya gestión esté libro [sic] *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* [sic] *en el caso* [sic] *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 S.A.S. que presente su colaboración para que Facebook Inc. y Facebook Ireland Limited cumplan las instrucciones y órdenes impartidas por esta Superintendencia* [sic] *en esta resolución. (…)"*

SEGUNDO. Que la Resolución No. 1321 de 2019 fue notificada por aviso a Facebook Inc., el 18 de marzo de 2019, según certificación de la Secretaría General Ad-Hoc de esta superintendencia[2].

TERCERO. Que, por medio de comunicación 18-233402-15-00[3], Facebook Inc., presentó recurso de reposición y, en subsidio apelación en contra de la Resolución No. 1321 de 2019, con fundamento en los siguientes argumentos:

1. La recurrente manifiesta que, esta superintendencia no tiene jurisdicción para pronunciarse sobre Facebook y sus servicios. Pues, además de que el domicilio de Facebook es en Estados Unidos, no realiza ninguna actividad en Colombia. Razón por la cual, esta entidad carece de autoridad para imponer sobre Facebook órdenes administrativas como las de la Resolución No. 1321 de 2019. Máxime, cuando no ha ocurrido ninguna afectación a usuarios colombianos del servicio de la plataforma de Facebook, que deba ser notificada con relación a la presunta transferencia de Datos de usuarios a *Cambridge Analytica,* por parte de un tercero desarrollador de aplicaciones en vulneración de la política de Facebook.

2. También declara que, el acto administrativo recurrido se profirió sin el lleno de los requisitos legales exigidos por el debido proceso.

   a. Asimismo, afirma que en relación con las garantías procesales, esta entidad no le otorgó una oportunidad adecuada para hacer declaraciones de defensa frente a la Resolución No. 1321 de 2019. Y debido a esto, vulneró su derecho al debido proceso.

   b. Considera que, esta entidad no cumplió con el procedimiento establecido en el artículo 47 de la Ley 1437 de 2011, a fin de proferir la Resolución No. 1321 de 2019.

   c. Alega que esta superintendencia vulneró el principio según el cual las entidades públicas pueden actuar conforme con lo que la ley les autorice. Y aduce:

---

[2] Folios 493-530
[3] Folios 531, carpeta 2.

"(…) Las medidas preventivas únicamente pueden imponerse de forma temporal, conforme lo estipule la ley expresamente y solo cuando:

- *Las medidas propuestas no excedan lo que proporcionalmente, en vista del problema identificado, es necesario, y se impongan en igualdad de términos en comparación con otros sujetos a la ley aplicable;*
- *SI las medidas propuestas no se imponen o se implementen de forma tardía, se generarían graves daños y perjuicios (periculum in mora); y*
- *Siempre y cuando la SIC demuestre que su posición es discutible y/o tiene algún mérito (fumis boni iuris o apariencia del buen derecho).*

Las órdenes que la SIC [sic] *pretende imponer sobre Facebook y otros, no se basan en ninguna autoridad ni poder otorgado por la ley, ni tampoco son de carácter temporal.*

La autoridad de la SIC [sic] *de imponer medidas preventivas, como las de este caso, se limita a las circunstancias en las que una investigación se relacione a asuntos de competencia desleal y antimonopolio (…).*

(…)

La SIC [sic] *ignoró el requisito de primero abrir y completar una investigación específica para el asunto relevante, antes de proceder con la imposición de condiciones. Esto es lógico, ya que la SIC* [sic] *no puede conocer si las medidas que impondrá son verdaderamente necesarias o si serán efectivas si no las ha evaluado, o si no le ha brindado a la parte investigada la oportunidad de establecer las disposiciones o hacer comentarios sobre la efectividad e idoneidad de las disposiciones o hacer comentarios sobre la efectividad de los sistemas y controles de Facebook. La SIC* [sic] *no completó una investigación apropiada en este aspecto y, con sujeción a su adecuada competencia (la cual no se acepta ni admite), la SIC* [sic] *no tiene la facultad de imponer ninguna medida hasta que complete dicha investigación (…)".*

d. La recurrente aduce que, esta entidad vulneró la presunción de inocencia y el derecho a la defensa de Facebook al publicar, mediante una conferencia y un comunicado de prensa, el contenido de la Resolución No. 1321 de 2019, casi en su totalidad antes de darle la oportunidad de ejercer sus derechos a la defensa o permitirle el acceso adecuado a la decisión administrativa.

"(…) La Superintendencia [sic] *vulneró el derecho al debido proceso al publicar un acto administrativo que no era definitivo (en la medida en que a Facebook no se le había otorgado sus derecho a la defensa y a ser oído) y que, en el momento de la publicación (enero 28), no había sido notificado formalmente a Facebook. Como mínimo, la SIC* [sic] *debería notificar a Facebook antes de publicar la medida en la página web y/o en los medios. El incumplimiento por parte de la SIC* [sic] *en este sentido, vulneró los derechos al debido proceso de Facebook al publicar afirmaciones que no son exactas y que se han realizado sin escuchar los intereses de Facebook en cuanto a los hechos o la proporcionalidad de las medidas propuestas por la SIC* [sic]*".*

3. La recurrente expresa que esta autoridad no logró demostrar que las medidas de seguridad actuales de la plataforma de Facebook son insuficientes o inadecuadas para garantizar la seguridad de los Datos personales de los usuarios de Facebook.

"La SIC [sic] *no se basa en evidencia apropiada para respaldar sus conclusiones, ni de otra forma explica cómo los asuntos generales descritos en la Decisión* [sic] *1321/2019* [sic] *pueden relacionarse con la presunta transferencia de datos* [sic] *de usuarios a Cambridge Analytica por parte de un tercero desarrollador de aplicaciones vulnerando la política de Facebook.*

Como autoridad administrativa obligada a cumplir con los estándares del debido proceso, la SIC [sic] *debe en todo caso evidenciar las afirmaciones fácticas de las cuales pretende respaldarse (…)*

Adicionalmente, la evidencia empleada por la SIC [sic] *para respaldar la Decisión* [sic] *1321/2019* [sic] *es completamente inadecuada e inapropiada como base para el cuestionamiento de la idoneidad de las medidas de seguridad de la Plataforma de Facebook. La información incluida en la Decisión* [sic] *1321/2019* [sic] *es inexacta o desactualizada, o de otra forma se extrajo de fuentes de terceros, incluyendo informes de prensa e información pública sobre las investigaciones llevadas a cabo por autoridades extranjeras. Mediante la Decisión* [sic] *1321/2019* [sic] *la SIC* [sic] *se refiere a:*

(i) investigaciones [sic] *históricas de autoridades extranjeras relacionadas con eventos, los cuales en algunos casos ocurrieron hace más de 9 años, y que parecen no tener una relevancia continua con la presunta transferencia de datos* [sic] *de usuarios a Cambridge Analytica por parte de un tercero desarrollador de aplicaciones vulnerando la política de Facebook;*

(ii) investigaciones [sic] *actuales por parte de autoridades de privacidad de datos* [sic] *extranjeras, pero sin una explicación sobre los hechos sujetos a la investigación ni una explicación de cómo dichos hechos pueden relacionarse de forma general a los titulares* [sic] *de datos* [sic] *de la Plataforma* [sic] *de Facebook domiciliados o residentes en Colombia, o específicamente a la transferencia de los datos* [sic] *de usuarios a Cambridge Analytica; y*

(iii) varios artículos y publicaciones mediáticos, algunos a los que Facebook no tiene acceso, y sin respaldar la exactitud de los informes ni explicar la forma en la [sic] *se pudiesen haber empleado para llegar a la Decisión* [sic] *1321/2019* [sic].

(…)

La SIC [sic] *no puede concluir válidamente que Facebook no ha adoptado medidas de seguridad adecuadas o suficientes en relación a* [sic] *la plataforma de Facebook con base en informes de prensa sin haber buscado información de Facebook. La SIC* [sic] *tampoco puede imponer medidas (incluso si se caracterizan como cautelares) para mitigar una situación que no se ha establecido como existente de hecho o por ley.*

Si la SIC [sic] *investigase denuncias que indiquen que Facebook no ha adoptado salvaguardas de seguridad efectivas o suficientes en relación a los datos* [sic] *personales de usuarios de la Plataforma* [sic] *de Facebook en Colombia, estaría obligada a:*

(i) recolectar pruebas robustas y claras que respalden su posición que ha surgido una vulneración que afecte a los usuarios de la Plataforma [sic] *de Facebook ubicados en Colombia; y*

(ii) suministrar [sic] *dichas pruebas a Facebook y brindarle la oportunidad de oponerse a* [sic] *o contrariar dicha información.*

Los informes de prensa sobre las investigaciones emprendidas de conformidad con estándares legales extranjeros por parte de autoridades extranjeras en relación a [sic] *hechos distintos y a usuarios domiciliados fuera de Colombia no satisfacen los requisitos de grado de prueba en Colombia, y por lo tanto no pueden emplearse para justificar una orden como la que se impuso (…)*

Adicionalmente, los comunicados de prensa de Facebook no pueden ser empleados por la SIC como sustitución de una oportunidad de defensa o de otra forma para respaldar una presunta admisión de que la Plataforma [sic] *de Facebook no cuenta con medidas de seguridad suficientes o adecuadas. Por el contrario, los comunicados de prensa mencionados por la SIC* [sic] *respaldan la posición de Facebook de que ninguna vulneración de datos* [sic] *ha ocurrido, y comprueba una respuesta diligente ante el incidente Cambridge Analytica.*

La recurrente afirma que esta autoridad no siguió los procedimientos legales aplicables al transferir la evidencia de un expediente a otro. Asimismo aduce que *"(…) no le dio la oportunidad a Facebook de contradecir la evidencia que empleó para respaldar sus conclusiones respecto a la presunta falta de medidas de seguridad efectivas e idóneas dentro de la Plataforma* [sic] *de Facebook*. *La SIC* [sic] *también pretendió transferir la evidencia recolectada en otros expedientes al Expediente No. 18-233402 (el cual se relaciona con las medidas ordenadas por la Decisión* [sic] *1321/2019* [sic]*) sin seguir los procedimientos requeridos.*

La evidencia y los documentos investigados en el Expediente N. [sic] *(en el que la SIC* [sic] *sigue investigando una presunta vulneración del Artículo 17 (o) de la Ley 1581), Expediente No. 18-341022 (en el que la SIC* [sic] *sigue investigando un incidente relacionado con fotos en la Plataforma* [sic] *de Facebook) y el Expediente No. 18-257411 (en el que la SIC* [sic] *sigue investigando un incidente relacionado con la Plataforma* [sic] *de Facebook), fueron transferidos por parte de la SIC* [sic] *al Expediente No. 18-233402 (el cual se relaciona con las medidas de seguridad ordenadas por la Decisión 1321/2019). Esta acción ignora las formalidades procedimentales aplicables a los procesos contenciosos administrativos que se disponen expresamente en el Código de Procedimiento Administrativo y Contencioso Administrativo y por mandato expreso del Código General del Proceso (…)*

Por consiguiente, la evidencia puede transferirse de un expediente a otro únicamente si el derecho a la defensa en relación a [sic] *dicha evidencia ha sido agotado a plenitud (…) en un caso en el que una de las partes no tenga la oportunidad de intervenir u oponerse a la evidencia que será transferida, la autoridad competente deberá brindar la oportunidad a dicha parte de hacerlo. En este caso, dicha garantía no se le ofreció a Facebook, vulnerando su derecho fundamental constitucional al debido proceso, el cual incluye los derechos " a presentar pruebas y a controvertir las que se alleguen en su contra.*

La Secretaría General es la división competente para la certificación de que se siguieron las formalidades debidas en la transferencia de evidencia cuando la SIC considera apropiado transferir evidencia de un expediente a otro (…) no le dio a Facebook la oportunidad de contradecir la evidenciad [sic] *transferida de los*

expedientes No. 10-105923, No. 18-341022 y No. 18-257411 antes de expedir la Decisión [sic] *1321/2019* [sic].

> *La SIC* [sic] *debió revocar y desestimar la Decisión* [sic] *1321/2019* [sic] *en virtud de la no observancia de los derechos al debido proceso garantizados a Facebook y, particularmente, el derecho a la defensa en este caso."*

4. La recurrente argumenta que esta entidad cometió errores materiales y se basó en un mal entendimiento de los hechos para proferir la Resolución No. 1321 de 2019. Al respecto menciona lo siguiente:

"La Plataforma [sic] *de Facebook tiene medidas apropiadas para asegurar los datos* [sic] *de usuarios. Los terceros desarrolladores de aplicaciones han sido sometidos a controles desde la introducción de la Plataforma* [sic] *(…).*

No ha ocurrido ninguna afectación a usuarios colombianos del servicio de la plataforma de Facebook que deba ser notificado con relación a la presunta transferencia de datos [sic] *de usuarios a Cambridge Analytica por parte de un tercero desarrollador de aplicaciones en vulneración de la política de Facebook.*

(…) Facebook Login le permite a los terceros desarrolladores de aplicaciones solicitar el consentimiento de parte de los usuarios de Facebook para que sus aplicaciones accedan a categorías preespecificadas de datos [sic] *de usuario (…) El uso de Facebook Login está sujeto a los términos incluidos en la Política* [sic] *de la Plataforma* [sic] *de Facebook la cual prohíbe explícitamente la venta o el licenciamiento de datos* [sic] *de usuarios accedidos mediante Facebook con cualquier red de publicidad, agente de datos* [sic] *(data broker) u otro servicio relacionado con la publicidad o la monetización.*

"Thisisyourdigitallife" no obtuvo información sensible de las cuentas, como las contraseñas o la información financiera. El tercero desarrollador de aplicaciones en este caso únicamente obtuvo acceso a los datos [sic] *que los usuarios, quienes instalaron "Thisisyourdigitallife", aceptaron dar a la aplicación, y en caso de los amigos de dichos usuarios, los datos* [sic] *que dichos amigos publicaron en la Plataforma* [sic] *de Facebook y que pusieron a disposición del usuario que realizó la instalación (…)*

(…) Tanto el Dr. Kogan como Cambridge Analytica actuaron como terceros responsables de datos independientes en relación a [sic] *los datos* [sic] *que obtuvieron (esto es, ellos tuvieron control sobre y tomaron las decisiones de tratamiento* [sic] *en relación a dichos datos* [sic]*). Conforme se explicó anteriormente* [sic]*, Facebook no permitió ni aceptó dicha transferencia, y la misma ocurrió fuera de la Plataforma* [sic] *de Facebook en contravención de la Política* [sic] *de la Plataforma* [sic] *de Facebook.*

(…) Facebook actuó oportunamente para terminar los derechos de acceso de "Thisisyourdigitallife" para el uso de Facebook Login el 17 de diciembre de 2015. Facebook también evaluó que [sic] *acciones adicionales eran necesarias y aprobadas para hacer valer nuestra Política* [sic] *de la Plataforma* [sic] *de dicha época.*

(…) en abril de 2014 Facebook introdujo la Versión 2 de su interfaz de Programación de Facebook y otras consideraciones comerciales. Este cambio restringió substancialmente los datos [sic] *que las aplicaciones como la del Dr. Kogan podían acceder mediante Facebook Login (incluido una restricción al acceso a los datos* [sic] *de los amigos del instalador). Estas acciones evitarían que cualquier aplicación como la del Dr. Kogan lograra acceder a datos* [sic] *en esta medida hoy en día. Este cambio*

se asumió de forma plenamente voluntaria y no de conformidad al cumplimiento de una obligación legal para con los usuarios; este cambio tampoco fue generado por ninguna preocupación de que Facebook no estuviese cumpliendo con sus obligaciones legales. Todas las aplicaciones nuevas (esto es aquellas desplegadas en Facebook después de abril de 2014) se sometieron inmediatamente a todas las limitaciones (…). Para las aplicaciones preexistentes, se concedió un periodo de gracia de un año (hasta mayo de 2015) (…). Este periodo de gracias [sic] *se permitió para que los desarrolladores de aplicaciones pudieran realizar los cambios técnicos y, cuando fuese necesario, cambios de modelos comerciales o de producto que permitieran que las aplicaciones funcionaran con la API Gráfica V2".*

(…)

Sin realizar auditorías forenses, las cuales hemos retenido a solicitud de la Oficina de Comisionado de la Información del Reino Unido (…), no podemos saber con certeza que [sic] *datos* [sic] *transfirió el Dr. Kogan a SCL o qué usuarios fueron sometidos a una transferencia de datos* [sic] *por parte del Dr. Kogan a SCL (…). E incluso con estas auditorías, no sabemos que* [sic] *información encontraremos (particularmente si no existió una transferencia de ciertos tipos de datos* [sic] *a SCL). Sin embargo, como explicaremos más adelante, tanto en el registro público como la evidencia existente a nuestra disposición respaldan la conclusión de que el Dr. Kogan únicamente le suministró a SCL datos* [sic] *de usuarios de Facebook ubicados en los Estados Unidos. Aunque las cuentas del Dr. Kogan y la de SCL entran en conflicto en relación a* [sic] *algunos aspectos menores, ambas han mantenido en sus declaraciones a los reguladores y demás personas que el Dr. Kogan nunca le suministró a SCL datos* [sic] *de usuarios de Facebook ubicados fuera de los Estados Unidos, esto incluye a los usuarios ubicados en Colombia.*

(...)

En resumen, tanto el Dr. Kogan como SCL han declarado de forma reiterada y consistente que ningún dato [sic] *de usuarios de Facebook ubicados fuera de los Estados Unidos, (incluidos los usuarios ubicados en Colombia) se transfirió en ningún momento por parte de GSR a SCL. No existe evidencia que demuestre lo contrario en el registro público ni que halla* [sic] *llegado a nuestro conocimiento. Nuestras investigaciones internas (continuas) tampoco han encontrado evidencia en este aspecto ninguna evidencia* [sic] *que demuestre lo contrario.*

(...)

Aunque estos eventos no involucraron ningún tipo de violación de seguridad de la Plataforma [sic] *de Facebook legalmente notificable, debido a la publicidad que rodeaba estos eventos, Facebook concluyó que fue adecuado informar a los usuarios que la App* [sic] *pudo haber accedido a sus datos* [sic]*. Desde abril 9 de 2018, Facebook les mostró a los individuos un enlace en la parte superior de su News Feed de Facebook, el cual les permitió ver las aplicaciones que estaban usando y la información que compartieron con dichas aplicaciones. Las personas también podían eliminar aplicaciones que ya no deseaban. Como parte de este proceso, Facebook les notificó a los individuos si la App* [sic] *pudo haber accedido a su información.*

(...)

La misión de Facebook es darle poder a los individuos para que creen comunidades y por último unir al mundo. Las personas se unen a y utilizan Facebook para conectarse con amigos y familiares, para descubrir lo que está sucediendo en el

mundo y para compartir con otras personas lo que es importante para ellos. En consonancia con el motivo por el cual los individuos eligen usar Facebook, la posición adoptada a través de la plataforma es, y siempre ha sido, que el objeto de la información es compartirla, aunque los usuarios que eligen emplear el servicio pueden, y a menudo lo hacen, tienen controles de privacidad y los emplean como ellos prefieran (...)

Los usuarios se han unido a Facebook en cifras muy significativas precisamente porque desean participar en la cultura del intercambio, la cual es la base de la experiencia de Facebook y para disfrutar de las experiencias en línea sociales personalizadas que ofrece Facebook (...)

Aunque claramente busca educar e informar a los usuarios sobre la forma en la que la Plataforma [sic] *funciona, el papel final de Facebook es el de un intermediario en línea, facilitando un fácil y amigable intercambio libre de información de los usuarios. En términos generales, la decisión de qué y cuanto* [sic] *compartir, empleando las facilidades técnicas integradas en la plataforma, es una opción para los usuarios, no para Facebook.*

(...)

Desde el inicio fue claro que la introducción de las aplicaciones en la Plataforma [sic] *se diseñó para proveerle a los usuarios un acceso a proveedores de servicios terceros y para incrementar la socialización de la Plataforma* [sic] *– y que les permitiría a los usuarios compartir su información de Facebook de la manera que ellos eligieran, mejorando las experiencias en línea y los servicios a su disposición. Sin embargo, como discutiremos en más detalle más adelante, el intercambio de datos* [sic] *de usuarios con las aplicaciones siempre ha estado sujeto a un extenso control por parte de los usuarios y siempre ha existido una gran transparencia en materia de: (a) las circunstancias en las cuales los datos* [sic] *de usuarios pueden compartirse con las aplicaciones; y (b) la existencia y el carácter de los controles a disposición de los usuarios que desean regular dicho intercambio.*

(...)

- *"La recolección de datos* [sic] *por parte de aplicaciones de terceros es, y siempre ha sido, independiente de las actividades de recolección de datos* [sic] *de Facebook (por ejemplo, la recolección de datos con el fin de permitir una personalización del contenido en los servicios para sus usuarios), incluyendo la publicidad de la cual Facebook puede recibir pagos). Facebook no recolecta datos* [sic] *por sí mismo como resultado de un proceso de intercambio de datos* [sic] *de usuario a aplicación. El desarrollador de aplicaciones tercero relevante que solicita permiso de parte de los usuarios para recolectar datos* [sic] *es el que hace esto, y lo hace bajo su calidad exclusiva de controlador de datos* [sic] *independiente;*

- *Facebook no recibió pago alguno como resultado de la decisión por parte de los usuarios de compartir datos* [sic] *con aplicaciones de terceros vía Facebook Login durante el Periodo* [sic] *Relevante* [sic]*, y este sigue siendo el caso hoy en día;*

- *Desde la primera integración de las aplicaciones en la Plataforma, el intercambio de datos de usuario con aplicaciones de terceros mediante Facebook Login siempre ha ocurrido a instancias de los usuarios que desean*

instalar la aplicación relevante: es su decisión compartir la información con la aplicación lo cual resulta en la obtención de los datos [sic] *por parte de la aplicación;*

- *El papel de Facebook en relación al* [sic] *proceso que permite que las aplicaciones de terceros recolecten los datos de usuarios de Facebook siempre ha sido el de un intermediario en línea: técnicamente facilita las decisiones activas de intercambio de datos* [sic] *de sus usuarios. De hecho, el papel de Facebook es responder, de forma automatizada, a los comandos de intercambio de datos* [sic] *instruidos por parte de los usuarios en relación a* [sic] *los datos* [sic] *que los usuarios mismos controlan (...)*

- *El intercambio de datos de usuario a aplicación entendido correctamente siempre ha sido equivalente a una transacción de intercambio de datos* [sic] *privado entre el usuario y la aplicación: el papel de Facebook es proveer los recursos técnicos para que las partes ejecuten dicha transacción privada (recalcamos, de conformidad con las decisiones de los amigos afectados de los usuarios conforme a* [sic] *sus configuraciones de privacidad)*

(...)

- *La Política de Datos de Facebook les informó a los usuarios sobre la manera en la que sus datos* [sic] *pueden intercambiarse con aplicaciones de terceros, y lo que podrían hacer para controlar o evitar dicho intercambio.*

- *Facebook también provee esta información "en el producto" (esto es, mientras que un usuario utilizaba Facebook). Ejemplos de formas en las que dicha información se suministraban a los usuarios durante parte de o todo el periodo de tiempo en el que las aplicaciones utilizaban Facebook Login según la API Gráfica V1 incluyen: cuando un usuario nuevo se une a Facebook; cuando los usuarios instalaban aplicaciones en la Plataforma; en páginas existentes de Aplicaciones* [sic] *de usuarios y de Configuración de Privacidad; en la función Privacy Check-up; en la función de Privacy Shortcuts; en Privacy Basics y en el Centro de Ayuda. Esta información en el producto reforzó las políticas de Facebook y llamó la atención de los usuarios en relación a* [sic] *su capacidad de controlar el intercambio de su información con aplicaciones de terceros.*

- *Los comunicados públicos de Facebook también reforzaron el mensaje sobre el intercambio de datos* [sic] *de usuario a aplicación (...)*

- *Todo esto sin hacer referencia al hecho de que la mayoría de los usuarios de Facebook también estarían al tanto de la manera en que las aplicaciones pretenden recolectar datos* [sic]*, incluidos los datos de los amigos de dichos usuarios, en todo momento de conformidad con y con sujeción a las configuraciones de privacidad de dichos amigos, como resultado de sus experiencias directas con la interacción con aplicaciones en la Plataforma* [sic].

(...)

Asimismo, la Política de Datos durante el Periodo [sic] *Relevante* [sic] *(en ese entonces denominada la Política de Uso de Datos), informó a los usuarios que sus amigos de Facebook podrían compartir sus datos* [sic] *con las aplicaciones que dichos amigos usaran, y también dirigía a los usuarios a los controles que podrían emplear para decidir qué datos* [sic]*, si los hubiese, podrían compartirse con las aplicaciones a través* [sic] *sus amigos.*

(...)

La misma Política [sic] *de Datos* [sic] *también les suministra información adicional a los usuarios sobre la Plataforma* [sic] *de Facebook, los datos a las* [sic] *aplicaciones de terceros pueden pedir autorización* [sic] *para acceder, las formas en las que dichas aplicaciones pueden utilizar los datos y las opciones que los usuarios tienen para controlar los datos a los que las aplicaciones pueden acceder.*

5. Facebook considera que todos los usuarios aceptaron válidamente que sus Datos se compartieran con aplicaciones de terceros empleando Facebook Login en virtud de que, a su juicio:

    a. Existía una transparencia significativa en relación con la operación de aplicaciones de terceros en la Plataforma. Pues, la forma en la que estas aplicaciones podrían buscar acceder a los Datos relacionados con los usuarios que instalaban la aplicación y sus amigos mediante Facebook Login, y lo que todos los usuarios de Facebook podían hacer para controlar el intercambio de sus Datos con aplicaciones de terceros;
    b. Los usuarios podían ejercer control sobre la medida en la que sus Datos se compartían con aplicaciones de terceros, incluyendo sus amigos, mediante los controles de privacidad;
    c. Las aplicaciones de terceros, les explicaban a los usuarios la información a la que deseaban acceder, y después únicamente permitirían conocer la información que los usuarios que realizaban la instalación elegían proveer a dichas aplicaciones.

    Para la recurrente, lo anterior es consonante con su papel como *"intermediario en línea"*, al facilitar las decisiones de los usuarios en relación clon los Datos en su posesión que los mismos deseaban compartir con las aplicaciones que utilizaban.

6. Facebook manifiesta que, su Programa de Privacidad es un marco integrado y completo con dos objetivos globales: i) abordar riesgos de privacidad relacionados con el desarrollo, la gestión y el uso de productos nuevos y existentes, y 2. Proteger la información que Facebook recibe de sus usuarios o aquella relacionada con los mismos. Asimismo, afirma que su programa garantiza que los controles de privacidad funcionen adecuadamente, que las declaraciones de privacidad sean claras y precisas y que la compañía aborde proactivamente los riesgos emergentes en materia de privacidad. De igual manera, informa que también opera un programa de cumplimiento robusto diseñado para detectar violaciones y adoptar respuestas graduadas y apropiadas.

    Al respecto aduce que, impone restricciones estrictas sobre cómo sus socios y terceros desarrolladores pueden usar y revelar la información de los usuarios.

    Además, manifiesta que a pesar de proveer a los anunciantes reportes sobre los tipos de personas que ven sus anuncios y cómo esos anuncios se desempeñan, Facebook no comparte información que identifica personalmente a los usuarios en dichos reportes.

    Asimismo la recurrente afirma que, i) aunque el presunto uso indebido de los Datos por parte de *Cambridge Analytic*a no involucró una violación de la seguridad de los Datos, resalta que el sistema y los controles que tiene, abordan problemas técnicos y mecánicos además de riesgos de terceros; ii) organiza varias protecciones para asegurarse de prevenir y abordar intentos de hallazgo de vulnerabilidades en los códigos desde varias perspectivas; y, iii) está comprometida con hallar, arreglar y

prevenir errores que puedan vulnerar la seguridad del sistema, para lo cual, trabaja para mejorar continuamente sus defensas, a fin de contrarrestar amenazas emergentes y seguir por encima de sus adversarios.

Petición

La recurrente solicita la revocatoria de la Resolución No. 1321 de 2019, en razón a que:

a. Esta entidad no tiene jurisdicción ni autoridad sobre Facebook o su plataforma.
b. El acto administrativo mencionado se profirió sin el cumplimiento de los estándares mínimos.
c. Esta autoridad además de cometer errores materiales, no demostró que las medidas de seguridad de la plataforma de Facebook son insuficientes o inadecuadas para garantizar la seguridad de sus usuarios.

CUARTO. Que a través de la Resolución No. 35800 de 12 de agosto de 2019, la Dirección de Investigación de Protección de Datos Personales resolvió el recurso de reposición y concedió la apelación.

QUINTO. Que de conformidad con lo establecido en el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, y con base en lo expuesto por la recurrente en el escrito de reposición y en subsidio apelación contra la Resolución No. 1321 del 24 de enero de 2019, se procede a resolver el recurso apelación interpuesto, de acuerdo con las siguientes,

CONSIDERACIONES DEL DESPACHO

1. **LA LEY 1581 DE 2012 ES APLICABLE A FACEBOOK INC. PORQUE RECOLECTA DATOS PERSONALES EN EL TERRITORIO DE LA REPÚBLICA DE COLOMBIA A TRAVÉS DE *COOKIES* QUE INSTALA EN LOS EQUIPOS O DISPOSITIVOS DE LAS PERSONAS RESIDENTES O DOMICILIADAS EN COLOMBIA.**

El artículo 2 de la Ley Estatutaria 1581 de 2012 dispone:

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

El término "Tratamiento" no sólo se menciona en el artículo 15[4] de la Constitución Política de la República de Colombia, sino que, es determinante para establecer el campo de aplicación de la citada ley, la cual lo define de la siguiente manera:

> ***Artículo 3. Definiciones.*** *Para los efectos de la presente ley, se entiende por:*
> *(…)*
> *g)* ***Tratamiento:*** *Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."*

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

---

[4] El artículo 15 de la Constitución de la República de Colombia dice, entre otras, lo siguiente: " Todas las personas tienen derecho a (…)conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.(Subrayamos)

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

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

La Corte Constitucional, por su parte, en relación con el ámbito de aplicación de ese artículo señaló en la Sentencia C-748 de 2011[5]:

> *"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]*.*

Las *cookies* son una herramienta para, entre otras, recolectar Datos personales. En este sentido, señala Guerrero que las "*entidades públicas y privadas y particulares se hacen presentes en la Red y recaban igualmente datos de otros a distancia sirviéndose de páginas web, (…) y otras aplicaciones 'invisibles' como* ***cookies*** *o web bugs*"[7]. (Destacamos). Según Morón Lerma, las *cookies* son "*pequeños programas que identifican al usuario cada vez que entra a un servidor de información y que rastrean sus preferencias*". Precisa la autora que, "*el sucesivo envío de cookies y su conservación permite al emitente lograr una fotografía digital del internauta, conocer su dirección, gustos, preferencias o entretenimientos, pudiendo efectuar un rastreo completo de las actividades del usuario en la red*"[8]

Las *cookies* han sido catalogadas como *"la principal tecnología de rastreo utilizada para controlar a los usuarios en internet (…)"*[9]. Estas tecnologías son utilizadas para realizar "*operaciones invisibles*" y "*tratamientos invisibles*"[10] de Datos. En síntesis, en Internet se puede recolectar información de personas de cualquier parte del mundo a través de diferentes medios tecnológicos visibles e invisibles, conocidos o no por los Titulares de los Datos personales. Esta captura de información técnicamente puede efectuarse sin que la empresa recolectora de los Datos esté físicamente ubicada en el territorio de la persona

---

[5] Cfr. Corte Constitucional. Sentencia C-748 de 2011. Disponible en: http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm

[6] Cfr. Corte Constitucional. Sentencia C-748 de 2011. Consideración 2.4.4.

[7] GUERRERO PICÓ, María del Carmen. 2006. El impacto de internet en el Derecho Fundamental a la Protección de Datos de carácter personal. Primera ed. Navarra: Thomson Civitas. p 25

[8] MORON LERMA, Esther. 2002. Internet y derecho penal: hacking y otras conductas ilícitas en la red. Segunda ed. Navarra, España: Aranzadi. p 33.

[9] GRUPO DE PROTECCION DE DATOS DEL ARTICULO 29. 2012. Dictamen 2/2010 sobre publicidad comportamental en línea. GT 171.

[10] El Grupo de Trabajo del artículo 29 expresó en 1999 su preocupación por "*todos los tipos de operaciones de tratamiento informático que se llevan a cabo actualmente en Internet a través del software y del hardware sin el conocimiento del interesado y que, por consiguiente, son "invisibles" para el mismo. Ejemplos típicos de este tipo de tratamiento invisible son el chattering en el nivel HTTP1, los hipervínculos automáticos a terceros, el contenido activo (como Java, ActiveX u otras tecnologías que ejecutan scripts en el cliente) y el mecanismo cookies en su aplicación actual en los navegadores usuales*" (GRUPO DE PROTECCION DE DATOS DEL ARTICULO 29. 1999. Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware. (5093/98/ES/final. WP 17), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp17es.pdf. . . P 2)

respecto de la cual se obtiene la información. De hecho, gracias a las tecnologías las empresas hoy en día tienen más presencia electrónica, que física.

Facebook Inc. reconoce que usa *cookies* para recolectar Datos en el territorio de la República de Colombia. En efecto, dicha empresa manifiesta que "*procesaremos los datos que recibamos a través de las cookies*", tal y como se evidencia en la siguiente imagen:

Es importante señalar que, otras autoridades de protección de Datos han concluido que las *cookies* son mecanismos que usan empresas extranjeras para instalarlas en los equipos de las personas de otros países y recolectar sus Datos.

En efecto, en España y Francia con ocasión a la investigación iniciada por varias autoridades de protección de Datos contra Google Inc.[11], dicha empresa argumentaba que no le aplica la ley local (legislación española) porque es una organización estadounidense cuyo medios que utiliza para el Tratamiento de Datos no están localizados dentro de la jurisdicción española y, por lo tanto, no entra dentro de los criterios de aplicación territorial que preceptúa el artículo 2.1.c) de la Ley Orgánica de Protección de Datos (LOPD)[12].

Frente a lo anterior, a finales de 2013 la Agencia Española de Protección de Datos (en adelante AEPD) concluyó lo siguiente con ocasión de una investigación que inició contra Google:

> "*En todo caso, (…),* ***la entidad Google Inc. recurre a medios situados en el territorio español con el fin de captar información en nuestro territorio (utilizando, entre otros, los equipos de los usuarios residentes en España para almacenar información de forma local a través de cookies y otros medios, así como ejecutando código en dichos dispositivos****), sin que la utilización de tales equipos para la recogida de datos se realice exclusivamente con fines de tránsito por el territorio de la Unión Europea, es decir, no se trata de equipos de transmisión, sino que* ***dichos equipos se emplean para la recogida y tratamiento de los datos****"[13]. (…)*. (Destacamos).

En sentido similar se pronunció la autoridad francesa de protección de Datos en enero de 2014[14].

---

[11] Las investigaciones surgieron por lo siguiente: El 24 de enero de 2012, Google Inc. anunció públicamente que iba a poner en práctica una nueva política de privacidad (NPPG) que regiría a partir del 1 de marzo de dicho año. Las Autoridades Europeas de Protección de Datos iniciaron acciones en el seno del Grupo del Artículo 29 (en adelante GT29) para analizar la NPPG y solicitaron a Google adoptar medidas para ajustar su nueva política a la regulación europea. Google no adoptó las recomendaciones del GT29. Dado lo anterior las autoridades de algunos países iniciaron investigaciones contra Google Inc.

[12] Google también manifestó lo siguiente: "*(...) debe tenerse presente que cuando la Directiva 95/46/CE fue elaborada no existía Internet ni, mucho menos, nada parecido a las cookies o los códigos ejecutados en los equipos de usuarios. El legislador pretendía aplicar la normativa comunitaria a aquellos responsables no comunitarios que tuviesen centros de proceso de datos en territorio de un Estado Miembro.*
El considerar los equipos de los usuarios como "medios" al servicio del responsable supone una interpretación forzada que conduce a una aplicación extraterritorial de las normas de los Estados Miembros de la UE que desborda los límites del sentido común." (Cfr. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución R/02892/2013 del 19 de diciembre de 2013. Procedimiento sancionador PS/00345/2013 instruido a las entidades Google Inc. y Google Spain, S.L. Madrid, España, p 12.).

[13] La AEPD concluyó lo siguiente: "*la Agencia Española de Protección de Datos también es competente para decidir sobre el tratamiento llevado a cabo por un responsable no establecido en territorio del Espacio Económico Europeo que ha utilizado en el tratamiento de datos medios situados en territorio español, por lo que debe concluirse, igualmente, que la LOPD es aplicable al presente supuesto y procedente la intervención de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 2.1.c) de la LOPD*" (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución R/02892/2013 del 19 de diciembre de 2013. Procedimiento sancionador PS/00345/2013 instruido a las entidades Google Inc. y Google Spain, S.L. Madrid, España).
La parte pertinente de la regulación española - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal- sobre su ámbito de aplicación dice lo siguiente:
"*Artículo 2 Ámbito de aplicación.*
1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.
Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:
a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
c) ***Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito****. (…)".* (Destacamos).

[14] Cfr. La CNIL consideró que las cookies que utiliza Google son un medio de tratamiento de datos y por ende le es aplicable la ley francesa (COMISIÓN NACIONAL DE INFORMÁTICA Y LIBERTADES (CNIL). Decisión 2013-420 del 3 de enero de 2014 contra la sociedad Google Inc. París, Francia). La ley francesa aplica a los tratamientos de datos, entre otros, efectuados por responsables no domiciliado en
territorio francés o en territorio de otro Estado miembro de la Comunidad Europea que recurra a mecanismos de tratamiento sobre el territorio francés salvo que aquellos medios tengan una finalidad exclusiva de transito sobre el territorio francés o el de otro Estado miembro de la Comunidad Europea. (Cfr. REPÚBLICA DE FRANCIA. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modificada por la Loi n° 2004-801 du 6 août 2004 relative à la protection

Sin perjuicio de lo mencionado consideramos pertinente referirnos a algunas definiciones de las *cookies* para reiterar que son mecanismos que instala Facebook Inc. en los equipos de las personas domiciliadas o residentes en la República de Colombia para recolectar en nuestro país Datos personales:

a. La Real Academia de la Lengua Española las define como, pequeños ficheros que se instalan en el disco duro o en el navegador del ordenador, tableta, teléfono inteligente o dispositivo equivalente con funciones de navegación a través de Internet y ayudan, entre otras cosas, a personalizar los servicios del titular de la web, facilitar la navegación y usabilidad a través de ella, obtener información agregada de los visitantes de la web, posibilitar la reproducción y visualización de contenido multimedia en la propia web, permitir elementos de interactuación entre el usuario y la web o habilitar herramientas de seguridad[15].

b. Google, las define como, un archivo pequeño que se guarda en las computadoras de las personas para ayudar a almacenar las preferencias y demás información que se utiliza en las páginas web que visitan[16].

c. La Comisión Federal del Comercio *(Federal Trade Comission[17] – FTC)* define una *cookie* como un pequeño archivo de texto que los sitios web instalan en su computadora.

   Este organismo también se refiere a los tipos generales de *cookies* que existen:

   "(...) Cookies de sesión única

   - *Facilitan la navegación de un sitio web.*
   - *Sólo registran información durante una visita a un sitio web y luego se borran.*
   - *Se activan de forma predeterminada para facilitar al máximo la navegación del sitio.*
   - *Se conocen también por el nombre de tecnologías Tier 1 bajo las pautas gubernamentales aplicables.*

   Cookies persistentes (multi-sesión)

   - ***Permanecen en su computadora y registran información cada vez que usted visita algunos sitios web.***

     Se almacenan en el disco duro de su computadora hasta que usted las elimine manualmente de una carpeta del navegador, o hasta que expiren, que puede ser

---

des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés).

[15] Recuperado de https://www.rae.es/info/cookies el 15 de marzo de 2020

[16] Recuperado de https://support.google.com/google-ads/answer/2407785?hl=es-419 el 15 de marzo de 2020

[17] *"A cookie is information saved by your web browser. When you visit a website, the site may place a cookie on your web browser so it can recognize your device in the future. If you return to that site later on, it can read that cookie to remember you from your last visit and keep track of you over time"*. Recuperado de https://www.ftc.gov/site-information/privacy-policy/internet-cookie el 15 de marzo de 2020.

"*A cookie is information saved by your web browser, the software program you use to visit the web. When you visit a website, the site might store a cookie so it can recognize your device in the future. Later if you return to that site, it can read that cookie to remember you from your last visit. By keeping track of you over time, cookies can be used to customize your browsing experience, or to deliver ads targeted to you".* Recuperado de https://www.consumer.ftc.gov/articles/0042-online-tracking el 15 de marzo de 2020.

De acuerdo con las anteriores definiciones podría afirmarse que, una *cookie* es información que se guarda en su navegador web. Esto ocurre cuando, se visita un sitio web, el cual, puede instalar una *cookie* en su navegador web para que pueda reconocer su dispositivo en el futuro. Así, al regresar a ese sitio virtual, la *cookie* le permitiría recordarlo a partir de su última visita y realizarle un seguimiento a lo largo del tiempo.

meses o años después de haber sido instaladas en su computadora (...)"[18]*.* (Destacamos).

d. El *Estudio sobre la privacidad de los datos y la seguridad de la información en las redes sociales online,* desarrolldo entre la Agencia Española de Protección de Datos y el Instituto Nacional de las Tecnologías de la Comunicación, se refieren al respecto así:

> ***"(...) La instalación y uso de "cookies" sin conocimiento del usuario.*** *Con frecuencia las redes sociales y plataformas análogas utilizan este tipo ficheros que tienen la posibilidad de almacenar determinada información sobre el usuario y su tipo de navegación a través de un sitio web.*
>
> *Estos ficheros se instalan en los equipos de los usuarios, de forma que resulta posible detectar el lugar desde el que accede el usuario, el tipo de dispositivo empleado (móvil o fijo) para el acceso, el tipo de contenidos accedidos, los lugares más visitados y las acciones habituales realizadas durante la navegación, así como el tiempo empleado en cada una de las páginas, entre otras muchas funcionalidades."*[19]*.*

e. La Agencia Española de Protección de Datos en su *Guía para el uso de las cookies* (página 11), las define como *"cualquier tipo de dispositivo de almacenamiento y recuperación de datos que se utilice en el equipo terminal de un usuario con la finalidad de almacenar información y recuperar la información ya almacenada"*

Dicha autoridad ha señalado que, para identificar a los usuarios se utilizan diferentes técnicas de seguimiento, las más conocidas son las *cookies*, es decir, ficheros almacenados en el ordenador del usuario que crea la propia página web del proveedor de servicios y que son utilizados posteriormente con diversas finalidades, como mejorar la experiencia del mismo con su navegador web, o estudiar la estadística de uso del sitio web por los usuarios, pero, también son utilizados con otras finalidades como es el perfilado de estos"[20]*.*

Igualmente, la misma Agencia junto con el Instituto Nacional de las Tecnologías de la Comunicación han expresado que, *"La instalación y uso de "cookies"* permiten *"a la plataforma conocer cuál es la actividad del usuario dentro de la misma. Mediante estas herramientas, las redes sociales pueden conocer el lugar desde el que el usuario accede, el tiempo de conexión, el dispositivo desde el que accede (fijo o móvil), el sistema operativo utilizado, los sitios más visitados dentro de una página web, el número de clicks realizados, e infinidad de datos respecto al desarrollo de la vida del usuario dentro de la red"*[21]*.*

f. El *Berkman Klein Center for Internet & Society* de la Universidad de Harvard, pone de presente que las *cookies* han sido objeto de críticas porque pueden utilizarse como un mecanismo para recopilar de forma invisible información sobre los hábitos de navegación del usuario con fines de *marketing*[22].

---

[18] Recuperado de https://www.ftc.gov/es/informacion-sobre-el-sitio/politica-de-privacidad/cookies-de-internet-0 el 15 de marzo de 2020

[19] Estudio sobre la privacidad de los datos y la seguridad de la información en las redes sociales online*. Página 98.* Edición febrero de 2009. Agencia Española de Protección de Datos y el Instituto Nacional de las Tecnologías de la Comunicación.

[20] ANÁLISIS DE LOS FLUJOS DE INFORMACIÓN EN ANDROID HERRAMIENTAS PARA EL CUMPLIMIENTO DE LA RESPONSABILIDAD PROACTIVA**.** Agencia Española de Protección de Datos Personales y Universidad Politécnica de Madrid, 7 de marzo de 2019. Página 3

[21] Estudio sobre la privacidad de los datos y la seguridad de la información en las redes sociales online*.* Páginas 11 y 12. Edición febrero de 2009. Agencia Española de Protección de Datos Personales y el Instituto Nacional de las Tecnologías de la Comunicación.

[22] "*Cookies are a mechanism by which a web server and a web browser can jointly "remember" information within or between browsing sessions. The web server sends a cookie containing some information to your browser, which may record it on your hard drive. When you next visit the website, that cookie is sent back to the web server. Cookies are useful because*

g. Por su parte, Facebook Inc, en su página web define estas herramientas como *"pequeños fragmentos de texto que se utilizan para almacenar información en navegadores web. Se utilizan para almacenar y recibir identificadores y otros datos en computadoras, teléfonos y otros dispositivos. Otras tecnologías, incluidos los datos que almacenamos en tu navegador web o dispositivo, los identificadores asociados a tu dispositivo y otros programas, se utilizan con fines similares. A los efectos de esta política, todas estas tecnologías reciben el nombre de "cookies"*[23].

Asimismo afirma, *"Utilizamos cookies si tienes una cuenta de Facebook, utilizas los Productos de Facebook, incluidos nuestro sitio web y nuestras aplicaciones, o visitas otros sitios web y otras aplicaciones que usan los Productos de Facebook, incluidos el botón "Me gusta" u otras tecnologías de Facebook. Las cookies permiten a Facebook ofrecerte los Productos de Facebook y entender la información que recibimos sobre ti, incluida la información sobre cómo usas los demás sitios web y aplicaciones o si te registraste o iniciaste sesión en ellos"*[24].

h. De otro lado, esta autoridad por medio del escrito 16-172268- -00001 definió las *cookies* como *"(...) archivos que recogen información a través de una página web sobre los hábitos de navegación de un usuario o de su equipo y eventualmente podrían conformar una base de datos de acuerdo a la definición legal de la Ley 1581 de 2012 al recolectar datos personales conforme a las características que jurisprudencialmente se han mencionado anteriormente; caso en el cual, el responsable deberá ceñirse por las normas sobre protección de datos vigentes en Colombia, en especial la aplicación de los principios rectores para la administración de datos, consagrados en el artículo 4 de la Ley 1581 de 2012 (...)".*

En el mismo escrito se da respuesta afirmativa al interrogante, *"(...) ¿se puede considerar como Tratamiento de Datos Personales, de acuerdo al literal g) del artículo 3 de la Ley Estatuaria 1581 de 2012, el uso de cookies, es decir, el envío de ficheros (pequeños archivos de datos de texto) por parte de un servidor web a un navegador para registrar las actividades del usuario en el sitio web? (...)"* , en los siguientes términos:

"(...) el tratamiento [sic] *se refiere a la utilización, recolección, almacenamiento, circulación y supresión de los datos* [sic] *personales que se encuentren registrados en cualquier base* [sic] *de datos* [sic] *o archivos por parte de entidades públicas o privadas y cuyo procesamiento sea utilizando medios tecnológicos o manuales".*

En suma, se concluye por parte de esta autoridad que, sin lugar a dudas, una *cookie* es un mecanismo que se instala en los equipos o dispositivos (bien sea celular, computador portátil, u otro) de las personas residentes o domiciliadas en la República de Colombia con el objetivo de recolectar algunos de sus Datos.

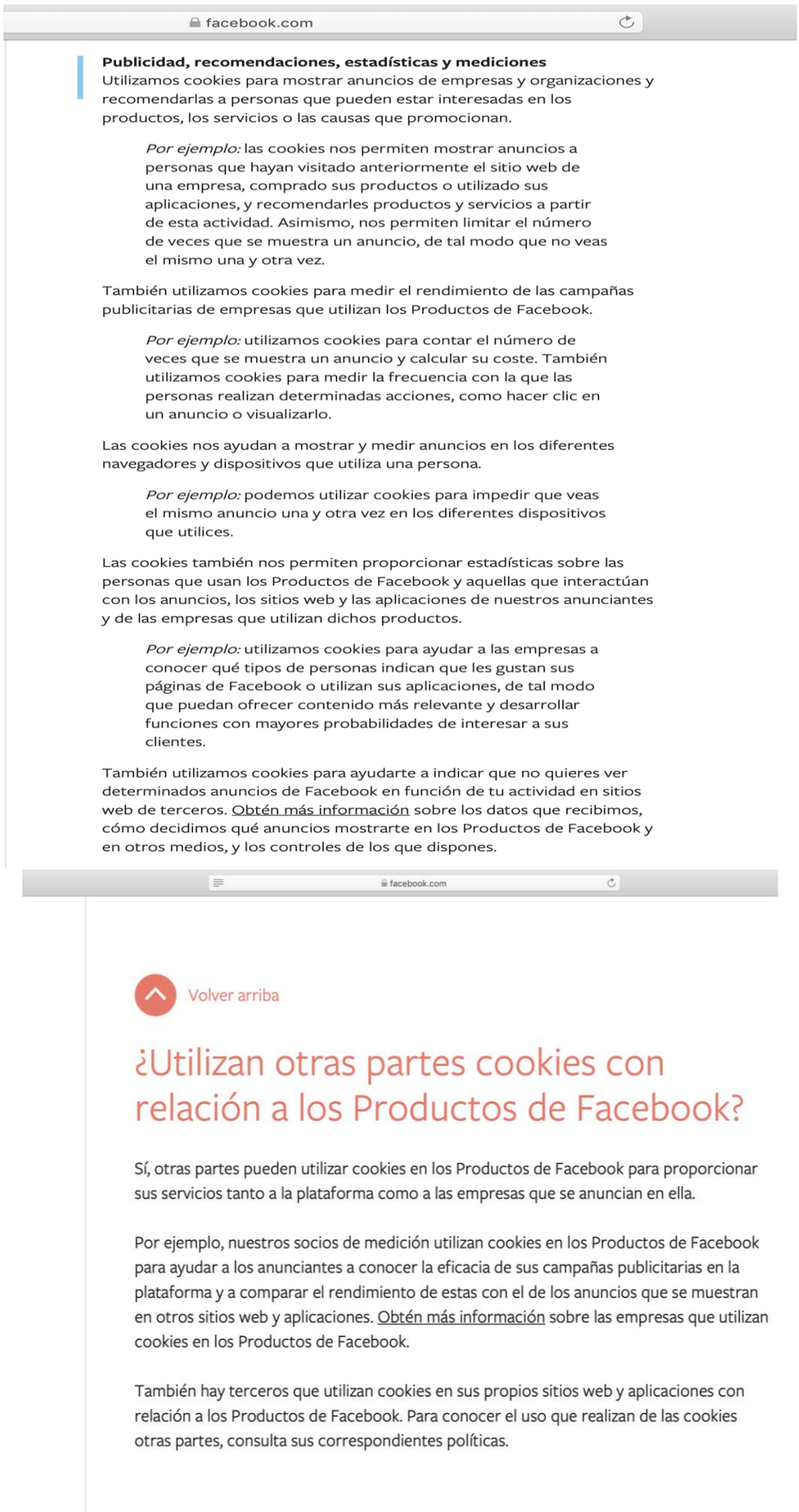
Reiteramos que, al realizar tanto el análisis del material probatorio, como de las páginas públicas de Facebook, se evidencia la siguiente información:

---

they can be used to improve the user experience. However, cookies have been subject to criticism because they can be used as a mechanism for invisibly gathering information about user's browsing habits for marketing purposes". Recuperado de https://cyber.harvard.edu/about/privacy-policy el 15 de marzo de 2020.

[23] Recuperado de https://es-la.facebook.com/policies/cookies/ el 15 de marzo de 2020.
[24] *Ibidem*


facebook.com
facebook
Registrarte
¿Has olvidado los datos de la cuenta?
¿Por qué utilizamos cookies?
¿Dónde utilizamos las cookies?
¿Utilizan otras partes cookies con relación a los Productos de Facebook?
¿Cómo puedo controlar el uso que hace Facebook de las cookies para mostrarme anuncios?
Más recursos
Política de cookies para imprimir
Política de datos
Condiciones
Configuración de anuncios de Facebook
Aspectos básicos de la privacidad
Cookies y otras tecnologías de almacenamiento
Las cookies son pequeños fragmentos de texto que se utilizan para almacenar información sobre los navegadores web. Permiten almacenar y recibir identificadores e información adicional sobre ordenadores, teléfonos y otros dispositivos. También se utilizan con fines similares otras tecnologías, como los datos que almacenamos sobre los navegadores web o los dispositivos, los identificadores que se asocian a los dispositivos y otros tipos de software. A efectos de esta política, todas las tecnologías referidas reciben el nombre de "cookies".
Utilizamos cookies en los siguientes casos: si tienes una cuenta de Facebook, usas los Productos de Facebook (incluidos nuestro sitio web y nuestras aplicaciones) o visitas otros sitios web y aplicaciones que utilizan dichos productos (incluidos el botón "Me gusta" o las tecnologías de Facebook). Las cookies permiten a Facebook ofrecerte sus productos y nos ayudan a comprender la información que recibimos de ti, incluidos los datos sobre el uso que realizas de otros sitios web y aplicaciones, independientemente de si estás o no registrado o si has iniciado sesión en la plataforma.
En esta política se explica el uso que hacemos de las cookies y las opciones de las que dispones. Salvo que se indique lo contrario en el presente documento, procesaremos los datos que recibamos a través de las cookies conforme a la Política de datos.



facebook.com

Publicidad, recomendaciones, estadísticas y mediciones
Utilizamos cookies para mostrar anuncios de empresas y organizaciones y recomendarlas a personas que pueden estar interesadas en los productos, los servicios o las causas que promocionan.

Por ejemplo: las cookies nos permiten mostrar anuncios a personas que hayan visitado anteriormente el sitio web de una empresa, comprado sus productos o utilizado sus aplicaciones, y recomendarles productos y servicios a partir de esta actividad. Asimismo, nos permiten limitar el número de veces que se muestra un anuncio, de tal modo que no veas el mismo una y otra vez.

También utilizamos cookies para medir el rendimiento de las campañas publicitarias de empresas que utilizan los Productos de Facebook.

Por ejemplo: utilizamos cookies para contar el número de veces que se muestra un anuncio y calcular su coste. También utilizamos cookies para medir la frecuencia con la que las personas realizan determinadas acciones, como hacer clic en un anuncio o visualizarlo.

Las cookies nos ayudan a mostrar y medir anuncios en los diferentes navegadores y dispositivos que utiliza una persona.

Por ejemplo: podemos utilizar cookies para impedir que veas el mismo anuncio una y otra vez en los diferentes dispositivos que utilices.

Las cookies también nos permiten proporcionar estadísticas sobre las personas que usan los Productos de Facebook y aquellas que interactúan con los anuncios, los sitios web y las aplicaciones de nuestros anunciantes y de las empresas que utilizan dichos productos.

Por ejemplo: utilizamos cookies para ayudar a las empresas a conocer qué tipos de personas indican que les gustan sus páginas de Facebook o utilizan sus aplicaciones, de tal modo que puedan ofrecer contenido más relevante y desarrollar funciones con mayores probabilidades de interesar a sus clientes.

También utilizamos cookies para ayudarte a indicar que no quieres ver determinados anuncios de Facebook en función de tu actividad en sitios web de terceros. Obtén más información sobre los datos que recibimos, cómo decidimos qué anuncios mostrarte en los Productos de Facebook y en otros medios, y los controles de los que dispones.

facebook.com

Volver arriba

¿Utilizan otras partes cookies con relación a los Productos de Facebook?

Sí, otras partes pueden utilizar cookies en los Productos de Facebook para proporcionar sus servicios tanto a la plataforma como a las empresas que se anuncian en ella.

Por ejemplo, nuestros socios de medición utilizan cookies en los Productos de Facebook para ayudar a los anunciantes a conocer la eficacia de sus campañas publicitarias en la plataforma y a comparar el rendimiento de estas con el de los anuncios que se muestran en otros sitios web y aplicaciones. Obtén más información sobre las empresas que utilizan cookies en los Productos de Facebook.

También hay terceros que utilizan cookies en sus propios sitios web y aplicaciones con relación a los Productos de Facebook. Para conocer el uso que realizan de las cookies otras partes, consulta sus correspondientes políticas.

[25] Imágenes recuperadas el 24 de enero de 2020. Fuente: https://www.facebook.com/policy/cookies/

El Tratamiento de Datos personales que hace Facebook Inc. es complejo y ocurre en distintos momentos y espacios físicos. Sin embargo, esto no impide reafirmar que la recolección de Datos personales de los usuarios de la plataforma en Colombia sucede parcialmente, pero en muy alto grado, en el territorio de la República de Colombia.

2. CONTEXTO DE LA ORDEN IMPARTIDA

La Superintendencia de Industria y Comercio - SIC, ordenó a Facebook Colombia S.A.S., Facebook Inc., y Facebook Ireland Limited adoptar nuevas medidas y mejorar las existentes para garantizar la seguridad de los Datos personales de más de 31 millones de colombianos usuarios de dicha red social digital. La decisión se tomó mediante la Resolución No. 1321 de 24 de enero de 2019.

La orden impartida es de carácter PREVENTIVO, a fin de evitar que se afecte la seguridad de los Datos de los colombianos.

La SIC relató los principales hechos de los siguientes casos difundidos por la prensa internacional y que ponen de presente algunas fallas de seguridad de Facebook respecto del Tratamiento de Datos personales:

a) Del programa "*Facebook Platform"* y del caso *Cambridge Analytica*
b) De hurto de los *"tokens"* para acceder a las cuentas de los usuarios de Facebook
c) Del acceso no autorizado a fotografías de usuarios de Facebook

La SIC no solo tuvo en cuenta las publicaciones de los medios de comunicación sino también, las declaraciones de Facebook y las decisiones; solicitudes e informes emitidos 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 de Norteamérica; la Casa de los Comunes del Parlamento Canadiense y la orden de Acuerdo de Consentimiento con la Comisión Federal de Comercio de los Estados Unidos de Norteamérica.

1. La Comisión de Protección de Datos de Irlanda *(The Data Protection Commission of Ireland);*
2. La Comisión Federal de Comercio de los Estados Unidos de Norteamérica (*The Federal Trade Commission);*
3. La Oficina del Comisionado de Información de Gran Bretaña (*The Information Commissioner's Office, ICO);*
4. La Comisión Nacional de Informática y de las Libertades de Francia (*La Commission Nationale de l'informatique et des libertés, CNIL);*
5. La Autoridad de Protección de Datos de los Países Bajos (*Autoriteit Persoonsgegevens) -"Dutch DPA"-;*
6. La Oficina del Comisionado de Privacidad de Canadá *(The Office of the Privacy Commissioner of Canada" (OPC);*
7. La Oficina del Comisionado de Información de Australia *(The Office of the Australian Information Commissioner);*
8. La Oficina del Comisionado de Privacidad de Nueva Zelanda *(The Office of the Privacy Commissioner of New Zealand);*
9. La Oficina del Fiscal General del Distrito de Columbia, Estados Unidos de Norteamérica *(The Office of the Attorney General for the District of Columbia).*
10. La Agencia Española de Protección de Datos (AEPD).

De todo lo anterior, esta autoridad concluyó que:

En primer lugar, Facebook no adoptó 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 de protección de Datos personales en diferentes países y sus políticas de privacidad y, en algunos casos, sin contar con el consentimiento de los Titulares.

En segundo lugar, Facebook ha reconocido vulnerabilidades de seguridad que permitieron a terceros hurtar *"tokens"* de acceso a Facebook, que luego podrían emplearse para tomar el control de cuentas de usuarios.

Finalmente, **Facebook ha admitido que fallas en el *"Photo API"* generaron que terceros desarrolladores de aplicaciones, accedieran a gran cantidad de fotografías de alrededor de 5.6 millones de usuarios**, por el periodo comprendido entre el 13 y el 25 de septiembre de 2018.

Esta superintendencia recordó que Facebook es la red social digital con mayor número de usuarios en el mundo y en la República de Colombia. Por eso, para esta autoridad, Facebook tiene la enorme responsabilidad de garantizar la seguridad de la información de todos sus usuarios, lo cual la 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.

3. COMPETENCIA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DE ACUERDO CON LA LEY 1581 DE 2012. FUNCIONES DEL DESPACHO DEL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES

El artículo 19 de la Ley 1581 de 2012 dispone que, "*La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para* ***garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos*** *previstos en la presente ley*" (Destacamos).

A su vez, el artículo 21 de la misma ley, establece cuáles son las funciones que ejercerá esta superintendencia, con relación al Tratamiento de Datos personales:

> *"(…)*
>
> *b. Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas* [sic] *data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos;*
>
> *(…)*
>
> *e. Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley;*
>
> *(…)"*

Por su parte, el artículo 16 del Decreto 4886 de 26 de diciembre de 2011[26] establece las funciones del Superintendente Delegado para la Protección de Datos Personales, entre las cuales se destacan las siguientes:

[26] Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones.

"(…)

7. Decidir los recursos de reposición y las solicitudes de revocatoria directa que se interpongan contra los actos que expida, así como los de apelación que se interpongan contra los actos expedidos por la Dirección a su cargo.

(…)"

A. DEL ALCANCE DEL TRATAMIENTO DE DATOS PERSONALES Y DEL MANDATO CONSTITUCIONAL DEL ARTÍCULO 15 PARA QUE EN CUALQUIER ACTIVIDAD SOBRE DATOS PERSONALES SE RESPETEN LA LIBERTAD Y DEMÁS GARANTÍAS CONSAGRADAS EN LA CONSTITUCIÓN POLÍTICA NACIONAL DE LA REPÚBLICA DE COLOMBIA

De cardinal importancia resulta establecer que, en el presente caso estamos frente al cumplimiento de exigencias de naturaleza constitucional referidas al Derecho Fundamental al debido Tratamiento de los Datos personales de los ciudadanos.

En efecto, el artículo 15 de la Constitución Política Nacional no solo establece el derecho que tienen, *"todas las personas (…) a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas*", sino que es tajante en exigir que:

> ***En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución."*** (Destacamos y subrayamos)

Con fundamento en lo anterior, se expidió la Ley Estatutaria 1581 de 2012 que desarrolla, entre otras, el citado derecho constitucional de naturaleza fundamental. En dicha ley se define **Tratamiento** como:

> *"**cualquier operación o conjunto de operaciones sobre datos*** [sic] ***personales**, tales como la recolección, almacenamiento, uso, circulación o supresión."*[27]

Esta expresión es de uso "técnico" en el ámbito de los Datos personales y es de tal importancia que, como se observa, ha sido incluida en el artículo 15 de nuestra Constitución Política. Y es así porque, determina el campo de acción de la Ley 1581 de 2012 en la medida que, salvo algunas excepciones, cualquier actividad que se realice, a través de medios manuales[28] o tecnológicos, con o sobre Datos personales debe observar unas reglas establecidas en la citada ley.

Nótese que la definición de Tratamiento tiene las siguientes características:

En primer lugar, es omnicomprensiva porque incluye toda actividad, operación o conjunto de operaciones sobre Datos personales. Además, no se limita a los ejemplos enunciativos del citado concepto legal sino que abarca cualquier otra como, entre otras, la publicidad o el *marketing* que involucre directa o indirectamente el uso, almacenamiento o circulación de Datos personales.

Sobre este punto, la Corte Constitucional señaló lo siguiente en el numeral 2.5.9. de la Sentencia C-748 de 2011 "*lo que se pretende con este proyecto es que **todas las***

---

[27] Cfr. Literal g) del artículo 4.

[28] Para la Corte Constitucional, *"no es válido argumentar que la ley de protección de datos personales cobija exclusivamente el tratamiento de datos que emplean las nuevas tecnologías de la información, dejando por fuera las bases de datos manuales, lo que resultaría ilógico, puesto que precisamente lo que se pretende con este proyecto es que todas las operaciones o conjunto de operaciones con los datos [sic] personales quede regulada por las disposiciones del proyecto de ley en mención, con las salvedades que serán analizadas en otro apartado de esta providencia".* Sentencia C-748 de 2011, numeral 2.5.9.

operaciones o conjunto de operaciones con los datos [sic] ***personales quede regulada por las disposiciones del proyecto de ley en mención****, con las salvedades que serán analizadas en otro apartado de esta providencia*". (Destacamos).

En segundo lugar, la operación o conjunto de operaciones sobre Datos personales puede ser realizada directa o indirectamente por una o varias personas de forma tal que, en un Tratamiento de Datos personales pueden existir varios Responsables o corresponsables.

Debe precisarse que, no es necesario que todas las etapas del Tratamiento las realice una misma empresa u organismo. Por ejemplo, si dentro de una organización se quiere recolectar y tratar Datos para fines de publicidad y/o *marketing*, es factible que unas actividades –*recolección, almacenamiento, análisis*- las realice un sujeto, y otras –*comercialización, venta, publicidad*- la efectúe otro que también haga parte de la misma organización. Al final, es un Tratamiento diseñado por una organización en la que se divide el trabajo para alcanzar ciertos objetivos pero, al final, unos y otros son Responsables y corresponsables del Tratamiento de Datos personales.

En tercer lugar, es neutral tecnológica y temáticamente porque cobija el Tratamiento realizado mediante cualquier medio físico o electrónico y para cualquier tema.

B. FACEBOOK INC. EN CONCURSO CON FACEBOOK COLOMBIA S.A.S. Y FACEBOOK IRELAND LIMITED., TIENEN LA OBLIGACIÓN DE CUMPLIR LA LEGISLACIÓN COLOMBIANA, ASÍ COMO LAS ÓRDENES Y REQUERIMIENTOS DE ESTA AUTORIDAD, EN CUMPLIMIENTO DE LA LEY 1581 DE 2012

En el escrito del recurso bajo estudio Facebook Inc. argumenta que esta autoridad no tiene ninguna jurisdicción sobre esa compañía. Por lo que, no puede pronunciarse sobre ella, ni los servicios que ofrece. Asimismo aduce que, lo anterior se reafirma porque no realiza ninguna actividad comercial en Colombia, y su domicilio está en Estados Unidos. Este punto se desarrollará en detalle más adelante.

Nuestra Constitución Política Nacional establece:

> Artículo 4 *"(…) Es deber de los nacionales y de los extranjeros en Colombia acatar la Constitución y las leyes, y respetar y obedecer a las autoridades"*[29]*.*
>
> Artículo 333 *"(…) La actividad económica y la iniciativa privada son libres, dentro de los límites del bien común. Para su ejercicio, nadie podrá exigir permisos previos ni requisitos, sin autorización de la ley. La libre competencia económica es un derecho de todos que supone responsabilidades*. **La empresa, como base del desarrollo, tiene una función social que implica obligaciones***.* (Destacamos).

Entonces, es la misma Constitución Política la que dispone el cumplimiento de la normatividad a los extranjeros que estén en este territorio. La cual, además, incluye el sometimiento a la ley en general, así como a las órdenes de autoridades administrativas, entre otras.

C. DE LA FACULTAD LEGAL PARA IMPONER LAS ÓRDENES CONTENIDAS EN LA RESOLUCIÓN NO. 1321 DE 2019

---

[29] "*Dicho reconocimiento genera al mismo tiempo la responsabilidad en cabeza del extranjero de atender cabal y estrictamente el cumplimiento de deberes y obligaciones que la misma normatividad consagra para todos los residentes en el territorio de la República pues, así lo establece, entre otras disposiciones, el artículo 4o. inciso segundo de la Carta (…)".* Corte Constitucional, Sentencia C-1259 de 2001

En el recurso interpuesto se argumentó que esta entidad no tiene las facultades legales para imponerle a Facebook Inc. las órdenes impartidas mediante la Resolución No. 1321 de 2019.

La afirmación de la recurrente es contraria a derecho porque la Ley Estatutaria 1581 de 2012 expresamente facultad a esta entidad a emitir órdenes o impartir instrucciones necesarias para que el Tratamiento de Datos personales se realice conforme con la ley.

En el artículo 19 de esa ley, se le otorgó competencia a esta entidad, a través de la Delegatura para la Protección de Datos Personales, para ejercer: "*(…) la vigilancia necesaria para garantizar que en el tratamiento* [sic] *de datos* [sic] *personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.*"

Asimismo, su artículo 21 determina cuáles funciones ejercerá la Superintendencia de Industria y Comercio, en virtud de la competencia conferida por el artículo 19 mencionado:

> *a. "Velar por el cumplimiento de la legislación en materia de protección de datos* [sic] *personales;*
>
> *b.* "*Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas,* ***ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas*** [sic] ***data****. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos* [sic]*, la rectificación, actualización o supresión de los mismos;*
>
> *(…)*
>
> *e. "****Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones*** *de los Responsables del Tratamiento y Encargados del Tratamiento* ***a las disposiciones previstas en la presente ley****;".* (Destacamos).

Visto lo anterior, contrario a lo afirmado por Facebook Inc. sí existen expresas y suficientes facultades legales para que esta superintendencia pueda impartir órdenes o instrucciones.

No sobra traer a colación que, el artículo 21 fue declarado exequible por la Corte Constitucional mediante la Sentencia C-748 de 2011, la cual en su numeral 2.20.3, expresa:

> *"Esta disposición enlista las funciones que ejercerá la nueva Delegatura de protección de datos personales. Al estudiar las funciones a ella asignadas, encuentra esta Sala que todas corresponden y despliegan los estándares internacionales establecidos sobre la autoridad de vigilancia. En efecto, desarrollan las funciones de vigilancia del cumplimiento de la normativa, de investigación y sanción por su incumplimiento, de vigilancia de la transferencia internacional de datos y de promoción de la protección de datos".*

En suma, la ley colombiana faculta a la SIC no solo para emitir órdenes o instrucciones sino para exigir el debido Tratamiento de los Datos personales. Por eso, esta entidad ha sido respetuosa del principio de legalidad y ha obrado conforme con lo establecido en el derecho colombiano.

D. LAS ÓRDENES NO SON SANCIONES. INAPLICABILIDAD DEL ARTÍCULO 47 DE LA LEY 1437 DE 2011 PARA PROCEDIMIENTOS ADMINISTRATIVOS SANCIONATORIOS

Facebook Inc. manifiesta que esta entidad no cumplió las etapas procesales establecidas en el artículo 47 de la Ley 1437 de 2011 a fin de proferir la Resolución No. 1321 de 2019.

Ese argumento de la recurrente también es abiertamente ilegal porque el artículo 47 de la Ley 1437 de 2011 es aplicable a los procedimientos administrativos de carácter sancionatorio. Y, en el presente caso, no estamos frente a uno de esa naturaleza porque **las órdenes no son sanciones.**

En efecto, las sanciones por infracción de la Ley Estatutaria 1581 de 2012 son únicamente las establecidas en su artículo 23, a saber:

> *"Artículo 23. Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:*
>
> *a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;*
>
> *b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;*
>
> *c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;*
>
> *d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;*
>
> *Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva."*

De la lectura del artículo anterior se constata que **las órdenes no son sanciones, motivo por el cual no es procedente surtir el procedimiento del precitado artículo 47, porque el mismo, se reitera, solo es aplicable a los procesos administrativos de carácter sancionatorio**.

Mediante la Resolución No. 1321 de 2019, la Dirección de Investigación de Datos Personales, emitió varias órdenes a la recurrente, pero, **de ninguna manera impuso una multa o alguna de las sanciones enunciadas en el artículo 23 de la Ley 1581 de 2012**.

Así las cosas, y en la medida en que en el presente caso no se trata de una actuación de carácter sancionatorio, es necesario recalcar que la presente actuación se siguió de acuerdo con el procedimiento pertinente, determinado en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

E. LAS COMPETENCIAS LEGALES DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO NO SE LIMITAN A IMPONER ÓRDENES EN ASUNTOS DE "ANTIMONOPOLIO O DE COMPETENCIA DESLEAL"

Según la recurrente, la facultad legal de esta superintendencia de imponer medidas preventivas como las de la resolución recurrida, se limita a las circunstancias en las que una investigación se relacione a asuntos de "*antimonopolio o de competencia desleal*"[30].

Al respecto, es preciso señalar que Facebook Inc. desconoce las funciones legales asignadas por la Ley 1581 de 2012 a esta entidad. En efecto, las órdenes de la Resolución No. 1321 de 2019 se emitieron en el ejercicio de las facultades legales conferidas expresamente por los artículos 19 y 21 de la Ley 1581 de 2012 y el artículo 17 del Decreto 4886 de 2011.

De esta forma, no es de recibo el argumento según el cual, esta autoridad no está facultada para imponer las órdenes contenidas en la resolución recurrida.

En el escrito bajo estudio se afirma que, las medidas preventivas solo se pueden imponer en temas de antimonopolio y competencia desleal. Sin embargo, este argumento no se sustenta por la recurrente. Adicionalmente, tampoco se explica por qué razón Facebook Inc. considera que esta superintendencia solo puede emitir medidas preventivas en las materias mencionadas, y no cuando pretende proteger el Derecho Fundamental a la Protección de Datos Personales y en general el cumplimiento de la Ley 1581 de 2012.

Esta superintendencia, según el literal a) del artículo 21 de la Ley 1581 de 2012, tiene la función de "*Velar por el cumplimiento de la legislación en materia de protección de datos* [sic] *personales*".

Velar, de acuerdo con la Real Academia de la Lengua Española significa, *"cuidar solícitamente de algo"*[31]. Es decir, que implica vigilar con cuidado y diligencia, a fin de identificar previamente los riesgos que pueden poner en peligro los Datos personales.

Por su parte, la potestad de esta superintendencia de "*impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley*"[32], no se limita a acciones de choque o posteriores a los daños causados a los Derechos Fundamentales protegidos por la Ley 1581 de 2012.

Cuando la norma se refiere a "*instrucciones*", no discrimina si las mismas son *ex ante* o *ex post* a la vulneración de la Ley 1581 de 2012. Dicho esto, es necesario reiterar el principio general de interpretación jurídica según el cual, donde la norma jurídica no difiere, está prohibido al intérprete diferenciar[33]. Siendo así, la norma citada permite impartir instrucciones de cualquier tipo, **preventivo**; de choque; de adecuación; con carácter reparatorio; etc., **siempre que las mismas tengan como finalidad el respeto a lo previsto en la Ley 1581 de 2012 y la defensa del Derecho Fundamental a la Protección de Datos Personales**.

En virtud de lo anterior, se concluye que, esta superintendencia sí puede impartir las medidas preventivas que considere necesarias con el propósito de evitar cualquier vulneración, daño o riesgo contra los derechos protegidos en la Ley 1581 de 2012.

El artículo 21 de la Ley 1581 de 2012 no se limita únicamente a funciones de sanción sobre las violaciones del Régimen General de Protección de Datos. Sino que, también, contiene **funciones de vigilancia y promoción**, entre otras. Lo anterior implica que, las funciones

---

[30] Folio 481 (reverso).
[31] Recuperado de https://dle.rae.es/?id=bTFZNAf|bTJiBaz|bTJnxpM el 13 de enero de 2020.
[32] Literal g) del artículo 21 de la Ley 1581 de 2012
[33] Corte Constitucional, Sentencia, C-703 de 2010, Magistrado Ponente, Mauricio González Cuervo, Considerando 5.2.7.4.1; Corte Constitucional, Sentencia C-317 de 2012, Magistrada Ponente María Victoria Calle, Considerando 3; Corte Constitucional, Sentencia C-087 de 2000, Magistrado Ponente Alfredo Beltrán Sierra, Considerando 5, literal b).

de la norma referida puedan ejercerse para prever la violación de cualquier disposición de la Ley 1581 de 2012.

Esta función legal contiene la posibilidad de "*ordenar las medidas*" que sean necesarias para hacer efectivo el Derecho Fundamental de *Habeas Data*. Esa norma no menciona las sanciones como equivocadamente lo interpreta la recurrente.

Ahora, la norma exige que esas medidas se impongan luego de una investigación, iniciada bien sea de oficio, o a petición de parte.

Es necesario aclarar que la investigación, **no siempre termina con una sanción**, tal y como sucede en el Procedimiento Administrativo Sancionatorio del artículo 47 de la Ley 1437 de 2011. También, puede finalizar con una orden o instrucción. Así pues, **el término "investigación", no puede equipararse a este procedimiento administrativo sancionatorio**. En este caso, la investigación se realizó dentro del expediente 18-233402 y siguió el Procedimiento Administrativo General, señalado en los artículos 34 y siguientes de la Ley 1437 de 2011.

4. DEBIDO PROCESO

En adición a lo anterior, se reitera que, la Superintendencia de Industria y Comercio obró dentro del marco de sus facultades legales para, de una parte, garantizar a las personas el Derecho Fundamental de la Protección de Datos Personales y, de otra, respetar el debido proceso en cabeza de Facebook Inc.

Al respecto, este Despacho advierte que, en ningún momento los actos o actuaciones de esta entidad en el curso de este proceso administrativo, han estado en contravía del derecho, como erróneamente lo infiere la recurrente. Esto, bajo el entendido de que en estas materias se tratan temas de magnitud constitucional y legal.

Esta Delegatura aplicó y respetó las garantías procesales necesarias, y emitió los actos administrativos a que hubo lugar. Los que, en ninguna circunstancia fueron arbitrarios. Por el contrario, lo que sí hizo esta autoridad, fue propender por la correcta aplicación de las normas y los principios que las fundamentan.

Igualmente, no es pasible dejar de lado que, en todo momento, esta autoridad dispuso las garantías procesales necesarias, y el correcto ejercicio y funcionamiento de la administración pública.

En vista de todo lo anterior, y luego de la plena evaluación de los elementos que hacen parte del expediente bajo estudio, es indiscutible concluir que esta entidad no desconoció el debido proceso para emitir una orden de naturaleza preventiva.

A. CUMPLIMIENTO DEL PROCEDIMIENTO FIJADO POR EL LEGISLADOR PARA IMPONER LAS ÓRDENES DE LA RESOLUCIÓN NO. 1321 DE 2019

En el recurso se argumentó que, para emitir el acto administrativo mencionado, debió desarrollarse el Procedimiento Administrativo Sancionatorio establecido en los artículos 47 y siguientes de la Ley 1437 de 2011.

Para esta autoridad, ese argumento debe rechazarse. Pues, como se mencionó, la Resolución No. 1321 de 2019 fue proferida bajo el Procedimiento Administrativo General regulado por los artículos 34 y siguientes de la Ley 1437 de 2011.

> *"**Las actuaciones administrativas se sujetarán al procedimiento administrativo común y principal que se establece en este Código**, sin perjuicio de los procedimientos administrativos regulados por **leyes especiales**. En lo no previsto en dichas leyes se aplicarán las disposiciones de esta Parte Primera del Código"*[34] (Destacamos).

En esta actuación, y al no existir un procedimiento administrativo especial que regule las actuaciones de esta delegatura, la Dirección de Investigación de Protección de Datos Personales, siguió, en cumplimiento de la norma transcrita, el procedimiento administrativo común.

Se reitera que, el procedimiento sancionatorio establecido en **el artículo 47 de la Ley 1437 de 2011, no se aplicó en esta actuación, en razón a que la finalidad de la investigación administrativa no consistía en la imposición de una multa o sanción.**

Con todo, se insiste en que las órdenes o instrucciones que fueron impartidas a través de la resolución recurrida tienen como único fin, prevenir el incumplimiento de la Ley 1581 de 2012 y el daño a los derechos fundamentales que la misma protege.

B. NO HUBO VIOLACIÓN DE DERECHOS EN NINGUNA INSTANCIA DE LA ACTUACIÓN ADMINISTRATIVA

En el escrito bajo estudio, la recurrente afirma que en relación con las garantías procesales, esta entidad no le otorgó una oportunidad adecuada para hacer declaraciones de defensa frente a la Resolución No. 1321 de 2019. Y debido a esto, esta superintendencia vulneró su derecho al debido proceso.

Adicionalmente, criticó que se hubiera dado a conocer ese acto administrativo a los medios de comunicación, antes que a ella. Y, antes de que pudiera ejercer sus derechos a la defensa o permitirle el acceso adecuado a la decisión administrativa.

Como se mencionó, el inicio de esta investigación fue debidamente informado[35] a la recurrente y ella se pronunció al respecto dando cumplimiento al inciso segundo del artículo 35 de la Ley 1437 de 2011:

> *"Cuando las autoridades procedan de oficio, los procedimientos administrativos únicamente podrán iniciarse mediante escrito, y por medio electrónico sólo cuando lo autoricen este Código o la ley, **debiendo informar de la iniciación de la actuación al interesado para el ejercicio del derecho de defensa**."* (negrita fuera del original).

Siendo así, la comunicación enviada le permitió a Facebook Inc. no solo conocer que se estaba desarrollando una investigación administrativa en su contra, también, garantizar su derecho de defensa y contradicción.

El ejercicio de las facultades que otorgan esos derechos, son potestativas para cada interesado. Por ejemplo, frente a la investigación de un hecho, el directamente involucrado puede guardar silencio; controvertir el hecho; solicitar la práctica de una prueba; etc., y cada una de esas actuaciones la hará dentro del ejercicio de sus derechos de defensa y contradicción. Es decir, las actuaciones garantizadas por esos derechos son optativas de cada administrado.

---

[34] Artículo 34 Ley 1437 de 2011.
[35] Mediante escrito 18-233402-3 de 1 de noviembre de 2018.

A su vez, en cumplimiento del artículo 36 de la Ley 1437 de 2011, el expediente físico y digital 18-233402 en todo momento, y desde el inicio de la investigación ha estado a disposición de la sociedad recurrente, para que sea consultado o se pronuncie sobre cualquier aspecto del mismo. Así como también, ha tenido la posibilidad de presentar oposiciones y de aportar y/o solicitar la práctica de las pruebas que considere pertinentes.

Este análisis concuerda con lo considerado por la Corte Constitucional en relación con el derecho de defensa:

> "*La jurisprudencia constitucional define el derecho a la defensa como la **'oportunidad reconocida a toda persona**, en el ámbito de cualquier proceso o actuación judicial o **administrativa**, de ser oída, de hacer valer las propias razones y argumentos, de controvertir, contradecir y objetar las pruebas en contra y de solicitar la práctica y evaluación de las que se estiman favorables, así como ejercitar los recursos que la ley otorga'*"[36] (Destacamos)

Así las cosas, vale la pena llamar la atención respecto de los siguientes aspectos:

a. Luego del inicio de la investigación administrativa que culminó con la expedición de la Resolución No. 1321 de 2019, era decisión de la sociedad recurrente manifestarse en el sentido que prefiriera. Como también, aportar y/o solicitar la práctica de pruebas que considerara relevantes para el desarrollo de la investigación. Para este efecto, el expediente siempre estuvo a disposición de Facebook Inc.

b. Los derechos de defensa y contradicción otorgan unas potestades a sus titulares, las cuales no son obligatorias, sino que, parten de la autonomía privada de cada uno de ellos.

c. La poca acción procesal de Facebook Inc. hasta antes de la expedición de la Resolución No. 1321 de 2019, pese a que se le informó del inicio de la actuación administrativa, además de que siempre tuvo acceso al expediente, no significa que esta entidad haya vulnerado sus derechos o que hubiese actuado de manera ilegal.

d. Facebook Inc. siempre tuvo oportunidad de expresar sus opiniones y de acceder al expediente. De igual manera, es libre de definir sus estrategias jurídicas y obrar conforme con las mismas. No obstante, si los resultados de la actuación administrativa no son los deseados por esa sociedad, no es dable endilgarle tal responsabilidad a esta entidad, y tampoco afirmar que la misma obró contrario a derecho.

Adicionalmente, los recursos de reposición y apelación interpuestos contra la resolución mencionada, son las formas establecidas por la Ley 1437 de 2011 para debatir las conclusiones del acto administrativo definitivo que pone fin a la investigación en curso. Esta posibilidad está en el artículo 74 de la Ley 1437 de 2011:

> "*Por regla general, contra los **actos definitivos procederán** los siguientes recursos: 1. El de reposición (…) 2. El de apelación (…).*" (Énfasis añadido).

Luego de emitido el acto administrativo, es la sociedad recurrente la que tiene la potestad -que no es obligatoria-, de interponer los recursos señalados en el artículo referido.

---

[36] Corte Constitucional, Sentencia T-018 de 2017, Magistrado Ponente Gabriel Eduardo Mendoza, Considerando 4.2; Corte constitucional, Sentencia C-025 de 2009, Magistrado Ponente Rodrigo Escobar Gil, Considerando 3.2.

Por medio del presente acto administrativo se analiza el recurso de apelación interpuesto por la sociedad y, ese hecho, desvirtúa el argumento relacionado con la falta de oportunidad de controvertir las conclusiones del acto recurrido.

Por último, respecto de la presunta violación de derechos fundamentales por la publicación de la Resolución No. 1321 de 2019 en la página *web* de esta autoridad, y en los medios de comunicación, es importante recordar lo establecido en el artículo 73 de la Ley 1437 de 2011:

> *"Cuando, a juicio de las autoridades, los actos administrativos de carácter particular afecten en forma directa e inmediata a terceros que no intervinieron en la actuación y de quienes se desconozca su domicilio, ordenarán publicar la parte resolutiva en la página electrónica de la entidad y en un medio masivo de comunicación en el territorio donde sea competente quien expidió las decisiones. En caso de ser conocido su domicilio se procederá a la notificación personal."*

Ahora, si se tiene en cuenta que la decisión impacta directa e inmediatamente a las más de 146.697 personas ubicadas en territorio colombiano que vieron afectados sus Datos por el caso de *Cambridge Analytica*, de acuerdo con la información que Facebook Ireland Limited remitió a la Dirección de Investigación de Protección de Datos Personales[37]. También, esa publicación fue razonable, en virtud de la importancia que tienen las órdenes impartidas para el grupo de usuarios de la plataforma Facebook en Colombia, que oscila alrededor de 15 millones de personas[38].

De otra parte, la citada publicación en la página web es consistente con el principio de divulgación proactiva previsto en el artículo 3 de la Ley 1712 de 2014[39], a saber:

> *"Principio de la divulgación proactiva de la información. El derecho de acceso a la información no radica únicamente en la obligación de dar respuesta a las peticiones de la sociedad, sino también en el deber de los sujetos obligados de promover y generar una cultura de transparencia, lo que conlleva* ***la obligación de publicar y divulgar documentos y archivos que plasman la actividad estatal y de interés público, de forma rutinaria y proactiva, actualizada, accesible y comprensible****, atendiendo a límites razonables del talento humano y recursos físicos y financieros".* (Destacamos)

No debe olvidarse que este caso es de enorme interés público, en virtud de que los hechos surgieron a partir del escándalo mundial sobre *Cambridge Analytica* y Facebook.

Con fundamento en lo anterior, se concluye que, esta entidad no violó ningún derecho de la recurrente al publicar la decisión recurrida, en la página *web* de la entidad y en los medios de comunicación, antes de hacer la notificación ordenada por la Ley 1437 de 2011[40]. Con todo, el 25 de enero de 2019 -un día después de fechada la resolución en mención- fue

---

[37] Folio 46.

[38] Ministerio de Tecnología de la Información y las Comunicaciones. "Colombia es uno de los países con más usuarios en redes sociales de la región". Disponible en: https://mintic.gov.co/portal/604/w3-article-2713.html?_noredirect=1
Vale aclarar que otras fuentes señalan que los usuarios de Facebook en Colombia oscilan entre 20 y 31 millones de persona. Al respecto ver: "Facebook supera los 20 millones de usuarios en Colombia." Publicado en: https://colombia-inn.com.co/facbeook-supera-los-20-millones-de-usuarios-en-colombia/ (consultado el 23 de enero de 2019); y Latamclick. Estadísticas de Facebook 2018 en América Latina. Disponible en: https://www.latamclick.com/estadisticas-de-facebook-america-latina-2018/ (consultado el 23 de enero de 2019).

[39] *Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.*

[40] La publicación se realizó en la URL: http://www.sic.gov.co/superindustria-exige-a-facebook-fortalecer-medidas-de-seguridad-para-proteger-datos-personales-de-mas-de-31-millones-de-colombianos

enviada la citación[41] para notificación personal del acto administrativo a Facebook Inc., en cumplimiento del artículo 68 de la Ley 1437 de 2011.

Es importante aclarar que, la publicación de la Resolución No. 1321 de 2019, no sustituyó la notificación correspondiente del acto administrativo. Los términos para interponer los recursos de ley, se contabilizaron desde la notificación legal que prevé la Ley 1437 de 2011, y no desde la publicación del acto en la página *web* de la entidad y en los medios de comunicación. Esto, reafirma el respeto de esta entidad por el debido proceso y los derechos de contradicción y defensa de la sociedad recurrente.

En síntesis, esta superintendencia cumplió a cabalidad el procedimiento legal aplicable a este tipo de investigaciones, sujetándose estrictamente al procedimiento administrativo común, sin incurrir en la violación del derecho de defensa o contradicción de la recurrente.

Se reitera que esta autoridad:

a. Comunicó el inicio de la investigación a Facebook Inc.;
b. Garantizó el derecho de la sociedad a ser oída, aportar y solicitar pruebas;
c. Garantizó el derecho de contradicción, con el análisis del recurso en cuestión; y
d. No violó ningún derecho al publicar, conforme con el artículo 73 de la Ley 1437 de 2011, la Resolución No. 1321 de 2019.

5. LA ORDEN IMPARTIDA NO REQUIERE QUE SE CAUSE UN DAÑO PORQUE SU OBJETIVO ES PREVENTIVO, NO REPARADOR NI SANCIONATORIO.

Facebook Inc. manifiesta que los Datos compartidos por el Dr. Kogan eran solo de usuarios de la plataforma ubicados en Estados Unidos. Sin embargo, esa afirmación es posterior a que la recurrente aceptara desconocer en realidad qué información tenía el Dr. Kogan, y cuál de esa información se compartió con *Elections Limited (SLC), Cambridge Analytica* y con *Global Science Research Ltd. (GSR).* Asimismo es incierto cuáles usuarios se vieron afectados por el acceso no autorizado a sus Datos personales[42].

Con base en lo anterior, es imposible concluir con certeza que no se afectaron Datos personales de usuarios de la Plataforma Facebook ubicados en Colombia. Según la información que reposa en el expediente, al inicio de esta investigación, proporcionada por la sociedad Facebook Ireland Limited (que pertenece al Grupo Facebook): **setenta y cuatro (74)** usuarios de la Plataforma ubicados en territorio colombiano instalaron la aplicación "*thisisyourdigitallife*", por medio de la cual, se accedió a su información personal y a la de los amigos de su perfil; y **ciento cuarenta y seis mil seiscientos noventa y siete (146.697) usuarios ubicados en Colombia** "*(…) fueron los potencialmente afectados (…)*"[43], como contactos de usuarios que instalaron la aplicación que accedió sin Autorización a sus Datos.

Facebook Ireland Limited, al dar a conocer lo anterior, también aclaró que:

i. Fue necesario determinar la ubicación a fin de determinar esas cifras;
ii. No se incluyeron los usuarios que cerraron su cuenta de Facebook luego de ocurrido el incidente; y
iii. Las cifras pueden ser inexactas porque pueden incluir más usuarios.

---

[41] Comunicación 18-233402-7 (folio 471). El aviso, con radicado 18-233402-14 de 13 de marzo de 2019 (folio 491) fue la forma de notificación del acto administrativo recurrido. Esto se certificó por parte de la Secretaría General Ad-Hoc de esta la Superintendencia de Industria y Comercio el 25 de abril de 2019, a través de escrito 18-233402-16 (folio 531).
[42] *Ibidem.*
[43] Folio 46.

Ahora, de acuerdo con los argumentos que presentó Facebook Inc. en el recurso ante las decisiones de las Autoridades de Protección de Datos Personales de España y la Región Administrativa Especial de Hong Kong, afirmó que no se afectaron Datos personales de usuarios ajenos al territorio de Estados Unidos. Sin embargo, al revisar la decisión de la Agencia Española de Protección de Datos sobre el incidente de *Cambridge Analytica*, se evidencia que el archivo realizado por esa Autoridad (en el procedimiento No. E/01873/2019) indica que cuarenta y cuatro (44) personas instalaron la aplicación en España y que fueron ciento treinta y seis mil novecientas cuarenta y uno (136.941) los usuarios ubicados en territorio español los que pudieron verse afectados por el acceso no autorizado a sus Datos[44]. El archivo se ordenó por prescripción de la potestad de investigación, bajo la Ley Orgánica 15 de 1999 que aplica en España.

Por su parte, la Oficina del Comisionado para la Protección de Datos Personales de la Región Administrativa Especial de Hong Kong concluyó que no hubo violación del régimen de protección de Datos en su territorio por el incidente de *Cambridge Analytica*. Pues, la oficina de Facebook en Hong Kong no es responsable del Tratamiento. Además no hay evidencia de que usuarios de la Plataforma de Facebook en Hong Kong hubieran sido afectados por el incidente (sin afirmar, en ningún momento, que haya evidencia de que no hubo usuarios afectados por el incidente de *Cambridge Analytica* por fuera del territorio estadounidense)[45].

Adicionalmente, a través del escrito 18-233402-29 de 6 de diciembre de 2019[46], la recurrente allegó una comunicación de un asesor legal externo que señala los hallazgos de la Oficina del Comisionado de Información en Reino Unido (ICO, por sus siglas en inglés, *Information Commissioner's Office*). Según la cual, ese organismo tampoco encontró evidencia que sugiriera que los Datos de usuarios colombianos hubieran sido objeto de transferencia[47]. Es importante tener en cuenta que esa información proviene de un asesor legal externo de Facebook Inc.

Esta autoridad aclara que, contrario a esa información, la Oficina del Comisionado de Información en Reino Unido señaló en la *Monetary Penalty Notice* (notificación de multa) de 24 de octubre de 2018, que la aplicación del Dr. Kogan fue usada por cerca de trescientos mil (300.000) usuarios de Facebook alrededor del mundo, entre los que se encuentran mil cuarenta (1.040) usuarios en Reino Unido[48]. Además, según esa autoridad los Datos

---

[44] *"En el presente caso la solución procedente en Derecho es el archivo de las actuaciones contra FACEBOOK y CAMBRDIGE ANALYTICA, en la medida en que los hechos objeto de análisis han prescrito (artículo 47 de la LOPD), y en atención a que si bien hubo 44 personas en España que se instalaron la aplicación "thisisyourdigitallife", y que hay 136.941 personas en España que, pese a no haberse instalado la aplicación, tenían amigos que sí se la habían instalado y su configuración de seguridad permitía el acceso de la aplicación a sus datos, lo cierto es que no se ha constatado que los datos de éstos hayan sido comunicados por GSR a CAMBRIDGE ANALYTICA. (…) En segundo lugar, respecto de la no constatación de que los hechos hayan afectado a usuarios españoles, dicha circunstancia obedece que tal como se indica en el punto 3 del antecedente segundo de la presente resolución, la entidad CAMBRDIGE ANALYTICA habría cesado su actividad impidiendo cualquier acción tendente a verificar que dispone o ha dispuesto de datos de carácter personal de usuarios españoles."*
Agencia Española de Protección de Datos. "Resolución de archivo de actuaciones". Procedimiento N° E/01873/2018. Punto V. Disponible en: https://www.aepd.es/es/documento/e-01873-2018.pdf

[45] Privacy Commissioner for Personal Data. "Privacy Commissioner Completed Compliance Check on Facebook and Cambridge Analytica Incidente". Hong Kong. 22 de agosto de 2018. Disponible en: https://www.pcpd.org.hk/english/news_events/media_statements/press_20180822b.html

[46] Folios 549 a 555.

[47] Folios 553 a 555.

[48] *"37. The App was used by some 300,000 Facebook users worldwide. Because the App was able to collect data about the Facebook friends of its users, the total number of individuals about whom the App collected personal data has been estimated by the Facebook Companies as being up to 87 million worldwide. The number of UK Facebook users who used the App has been stated by the Facebook Companies to be 1,040 (though the Facebook Companies have also stated that 1,765 individuals in Great Britain used the App). The total number of UK Facebook users about whom the App collected personal data has been estimated by the Facebook Companies as being at least 1 million".*
"37. La aplicación fue usada por cerca de 300,00 usuarios de Facebook alrededor del mundo. Ya que la aplicación era capaz de recolectar información acerca de los amigos de los usuarios que la habían instalado, el número total de personas sobre las cuales la aplicación recolectó datos personales ha sido calculada por las compañías de Facebook en cerca de 87 millones a nivel mundial. El número de usuarios de Facebook en Reino Unido que usaron la aplicación ha sido estimado por las compañías de Facebook en 1,040 (aunque las compañías de Facebook también han señalado que 1,765 personas

personales de por lo menos un millón (1’000.000) de usuarios de esa red digital en Reino Unido, fueron recolectados por medio de la aplicación[49].

Con la información citada en el recurso es insensato concluir que no hubo afectados por el incidente de *Cambridge Analytica* por fuera del territorio estadounidense. Tan es así, que la Agencia Española de Protección de Datos y la Oficina del Comisionado de Información en Reino Unido, determinaron que sí hubo afectados por ese incidente en esos países.

De esta manera, y con base en la información, adicional a la solicitada en la investigación a Facebook Ireland Limited, esta entidad considera que el argumento de Facebook Inc. en relación con la evidencia que supuestamente soporta firmemente la conclusión[50] según la cual los Datos compartidos por el Dr. Kogan eran solo de usuarios de la Plataforma de Facebook ubicados en Estados Unidos de Norteamérica, no está llamado a prosperar.

Si esta autoridad desconociera, la posible afectación de los Datos personales de los usuarios de la red social, ubicados en territorio colombiano, no solo sería irresponsable e imprudente, sino que, además, estaría incumpliendo con las obligaciones legales a su cargo, señaladas en el artículo 19 y 21 de la Ley 1581 de 2012.

En todo caso, nótese que la orden emitida es de carácter preventivo, no se trata de una sanción por causar daños a los Titulares de Datos ubicados en el territorio de la República de Colombia. Debe recordarse que la mejor forma de proteger un derecho es evitar su vulneración. Por esa razón, la orden tiene como propósito que Facebook Inc. mejore sus medidas de seguridad para evitar que se causen daños a las personas residentes o domiciliadas en Colombia.

6. NO SE VIOLÓ EL DERECHO FUNDAMENTAL DE DEFENSA NI SE OMITIERON LAS FORMALIDADES PROCESALES PARA INCORPORAR PRUEBAS DEL EXPEDIENTE 18-105923, EN EL EXPEDIENTE 18-233402

Facebook Inc. argumentó en el recurso que, esta superintendencia no siguió el procedimiento legal para incorporar información de las actuaciones administrativas con radicados 18-105923, 18-341022 y 18-257411 en el expediente 18-233402. Según este argumento, esta entidad debió aplicar el artículo 174 de la Ley 1564 de 2012 y también debió certificar, por medio de su Secretaría General, la transferencia de pruebas de acuerdo con lo establecido en el artículo 22 del Decreto 4886 de 2011.

Al respecto, esta autoridad considera que: i) en el expediente 18-233402, no hay ningún documento o prueba trasladada de las actuaciones 18-341022 y 18-257411; ii) no se aplica el artículo 174 de la Ley 1564 de 2012 a los documentos del expediente 18-105923, en razón a que el procedimiento administrativo común, que se aplica en esta actuación, se rige por los artículos 34 y siguientes de la Ley 1437 de 2011. Así, los documentos del expediente 18-105923 se incorporaron como pruebas documentales a esta actuación administrativa bajo el No. 18-233402.

Lo anterior, en virtud del artículo 40 de la Ley 1437 de 2011, el cual señala que son admisibles todos los medios de prueba señalados en el Código General del Proceso (artículo 165).

---

en Gran Bretaña usaron la aplicación). El número total de usuarios de Facebook en Reino Unido sobre los cuales la aplicación recolectó información personal ha sido estimado por las compañías de Facebook en cerca de 1 millón”. Information Commissioner’s Office (ICO). “Monetary Penalty Notice”. 24 de octubre de 2018. Considerando 37. Página 12. Disponible en: https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf

[49] *Ibidem.* Information Commissioner’s Office (ICO). “Monetary Penalty Notice”. 24 de octubre de 2018. Considerando 37. Página 12. Disponible en: https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf

[50] Folio 501.

Según el artículo 34 de la Ley 1437 de 2011, las actuaciones administrativas se sujetan al procedimiento común, sin perjuicio de las leyes especiales. Y, en lo no previsto en esas leyes, se aplica la primera parte del Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Sin embargo no se hace ninguna mención a la Ley 1564 de 2012.

Con todo, se cumplieron con los principios establecidos en el artículo 3 de la Ley 1437 de 2011, con el fin de incorporar los documentos de la actuación 18-105923 al expediente 18-233402:

i) de acuerdo con el principio de economía, las autoridades deben proceder con austeridad, optimizando el tiempo y los recursos;
ii) el de celeridad hace referencia a evitar las dilaciones injustificadas; y
iii) el de eficacia se refiere a que las autoridades deben buscar que los procedimientos logren su finalidad.

Conforme con lo anterior, esta entidad evitó volver a recolectar los documentos y demás información de la actuación 18-105923, en el expediente 18-233402, con el fin de no dilatar la decisión, ni aumentar los costos de tiempo y recursos públicos en el desarrollo del expediente 18-233402.

En suma, si esta entidad a través de otra investigación al mismo sujeto obligado, ya había reunido una información bajo el expediente 18-105923, no habría sido consecuente con los principios del artículo 3 de la Ley 1437 de 2011 realizar nuevamente la consecución de esos documentos en esta actuación.

Ahora bien, en este caso no es aplicable el artículo 174 de la Ley 1564 de 2012 que señala las garantías que se aplican al traslado de pruebas de expedientes en las materias regidas por el Código General del Proceso. Según el escrito bajo estudio, esa norma se aplica en virtud del artículo 211 de la Ley 1437 de 2011, la cual determina que en los "*procesos que se adelanten ante la Jurisdicción de lo Contencioso Administrativo, en lo que no esté expresamente regulado en este Código, se aplicarán en materia probatoria las normas del Código de Procedimiento Civil*". Sin embargo, en este caso la Superintendencia de Industria y Comercio no está ejerciendo funciones jurisdiccionales, razón por la cual no podría desarrollar un proceso judicial, que solo se podría adelantar ante la Jurisdicción Contencioso Administrativa. En este expediente esta autoridad está ejercicio funciones administrativas de inspección, vigilancia y control, de conformidad con lo establecido en los artículos 19 y 21 de la Ley 1581 de 2012.

El artículo 174 mencionado se aplica en procesos contenciosos en los que existen dos partes en conflicto, pero no en procedimientos administrativos inquisitivos como el administrativo común del caso. La norma, regula la prueba trasladada cuando se presenta contra una parte que no estuvo en audiencia o no la solicitó en otro proceso diferente a aquel en el cual se aduce. Se trata de casos en los cuales el Juez Contencioso Administrativo debe resolver un conflicto entre dos extremos procesales en conflicto, aquí sí aplicaría la remisión del artículo 211.

En el presente asunto el caso es totalmente diferente. Aquí no hay dos partes en conflicto, sino una entidad en ejercicio de funciones públicas, que analiza si debe o no impartir unas órdenes a un sujeto obligado.. De esta forma, el artículo 174 de la Ley 1564 de 2012 no es aplicable a este caso.

Ahora, si en gracia de discusión consideramos aplicable el artículo 174, tampoco se podría afirmar que no se cumplió con lo que exige la norma. Pues, según esta, la prueba practicada en un proceso se puede trasladar a otro proceso en copia y será apreciada sin más

formalidades, siempre que en el proceso inicial se hubiera practicado a petición de la parte contra la cual se aduce o con audiencia de ella. En caso contrario, la contradicción se debe surtir en el proceso destino. Adicionalmente, la norma señala que la valoración de la prueba y la definición de sus efectos procesales corresponde al juez ante el cual se presentan.

Si así fuera, en este caso las pruebas del expediente 18-105923 fueron practicadas en audiencia de Facebook Inc., pues, como se sabe, esa compañía también hace parte de la actuación 18-105923, en calidad de sujeto investigado. En esa actuación la recurrente intervino en diferentes ocasiones. Igual, bajo el expediente 18-233402 que corresponde a la presente investigación administrativa, Facebook Inc. ha tenido oportunidad de contradicción como se analizó. Por último, corresponde a esta autoridad, como juez según el artículo 174, definir la valoración y efectos procesales de las pruebas trasladadas. Como se ve, incluso con la aplicación del artículo 174 de la Ley 1564 de 2012, no es posible afirmar que esta entidad vulneró algún derecho de Facebook Inc. u omitió alguna etapa procesal.

Por último, con respecto a la supuesta obligación que tiene la Secretaria General de esta entidad de certificar la transferencia de documentos, es importante aclarar que en el artículo 22 del Decreto 4886 de 2011 no aparece esa función por ninguna parte. No existe en la ley, ni a nivel reglamentario, ninguna obligación en cabeza de la Secretaria General de la Superintendencia de Industria y Comercio de certificar la transferencia de documentos de una actuación administrativa a otra.

7. LA RESPONSABILIDAD DEMOSTRADA (*ACCOUNTABILITY*) FRENTE AL TRATAMIENTO DE DATOS PERSONALES LE IMPONE A FACEBOOK INC. EL DEBER DE PROBAR QUE HA ADOPTADO MEDIDAS APROPIADAS Y EFECTIVAS PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN DE SUS USUARIOS.

La recurrente expresa que esta autoridad no logró demostrar que las medidas de seguridad actuales de la plataforma de Facebook son insuficientes o inadecuadas para garantizar la seguridad de los Datos personales de los usuarios de Facebook.

> *"La SIC* [sic] *no se basa en evidencia apropiada para respaldar sus conclusiones, ni de otra forma explica cómo los asuntos generales descritos en la Decisión* [sic] *1321/2019* [sic] *pueden relacionarse con la presunta transferencia de datos* [sic] *de usuarios a Cambridge Analytica por parte de un tercero desarrollador de aplicaciones vulnerando la política de Facebook.*
>
> *Como autoridad administrativa obligada a cumplir con los estándares del debido proceso, la SIC* [sic] *debe en todo caso evidenciar las afirmaciones fácticas de las cuales pretende respaldarse (…)*
>
> *Adicionalmente, la evidencia empleada por la SIC* [sic] *para respaldar la Decisión* [sic] *1321/2019* [sic] *es completamente inadecuada e inapropiada como base para el cuestionamiento de la idoneidad de las medidas de seguridad de la Plataforma de Facebook. La información incluida en la Decisión* [sic] *1321/2019* [sic] *es inexacta o desactualizada, o de otra forma se extrajo de fuentes de terceros, incluyendo informes de prensa e información pública sobre las investigaciones llevadas a cabo por autoridades extranjeras. Mediante la Decisión* [sic] *1321/2019* [sic] *la SIC* [sic] *se refiere a:*
>
> *(i) investigaciones* [sic] *históricas de autoridades extranjeras relacionadas con eventos, los cuales en algunos casos ocurrieron hace más de 9 años, y que parecen no tener una relevancia continua con la presunta transferencia de datos* [sic] *de usuarios a Cambridge Analytica por parte de un tercero desarrollador de aplicaciones vulnerando la política de Facebook;*

(ii) investigaciones [sic] *actuales por parte de autoridades de privacidad de datos* [sic] *extranjeras, pero sin una explicación sobre los hechos sujetos a la investigación ni una explicación de cómo dichos hechos pueden relacionarse de forma general a los titulares* [sic] *de datos* [sic] *de la Plataforma* [sic] *de Facebook domiciliados o residentes en Colombia, o específicamente a la transferencia de los datos* [sic] *de usuarios a Cambridge Analytica; y*

(iii) varios artículos y publicaciones mediáticos, algunos a los que Facebook no tiene acceso, y sin respaldar la exactitud de los informes ni explicar la forma en la [sic] *se pudiesen haber empleado para llegar a la Decisión* [sic] *1321/2019* [sic].

(…)"

Posteriormente, en relación con su responsabilidad en el incidente de *Cambridge Analytic*a dio a conocer todas las medidas que ha implementado con el propósito de proteger la privacidad y los Datos personales de sus usuarios.

Sobre lo planteado por Facebook Inc. es necesario precisar lo siguiente:

En primer lugar, de confomidad con el principio de responsabilidad demostrada (accountability) "*los responsables* [sic] *del tratamiento* [sic] *de datos* [sic] *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*"[51] y en el Decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015). Por lo tanto, es a Facebook Inc, y no a esta entidad, a quien le corresponde probar que cuenta con medidas de seguridad apropiadas y efectivas para garantizar la seguridad en el Tratamiento de la información de sus millones de usuarios.

El término "***accountability***"[52], a pesar de tener diferentes significados, ha sido entendido en el campo de la protección de Datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, y la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente. 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. Se trata de una actividad constante, que exige demostrar un cumplimiento real y efectivo en la práctica de sus labores.

El Principio de Responsabilidad Demostrada –*accountability*- demanda implementar acciones de diversa naturaleza[53] 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 adopten medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia. Dichas acciones o medidas, deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los Datos personales.

Medidas "apropiadas" son aquellas ajustadas a las necesidades del Tratamiento de Datos. Y "efectivas", son las que permiten lograr el resultado o efecto que se desea o espera. En otras palabras, no se deben adoptar medidas inoperantes; inservibles; inanes o infructuosas.

---

[51] Cfr. Artículo 26 del Decreto 1377 de 2013 (Incorporado en el Decreto 1074 de 2015).
[52] Cfr. Grupo de trabajo de protección de datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 8.
[53] Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humana y de gestión. Asimismo involucran procesos y procedimientos con características propias en atención al objetivo que persiguen.

Solo se deben instaurar aquellas adecuadas; correctas; útiles; oportunas y eficientes con el propósito de cumplir los requerimientos legales para realizar Tratamiento de Datos personales.

El Principio de Responsabilidad Demostrada precisa menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre Tratamiento de Datos personales. Requiere apremiar acciones concretas por parte de las organizaciones para garantizar el debido Tratamiento de los Datos personales.

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. Como se ha manifestado, exige que se demuestre el cumplimiento real y efectivo en la práctica de 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* [sic] *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****"*[54]. (Énfasis añadido)

En segundo lugar, esta superintendencia debe reiterar que la información del incidente de *Cambridge Analytica*, sobre el acceso no autorizado a información personal de usuarios de Facebook y de los amigos de sus perfiles en su plataforma, ha sido recolectada de la misma información que empresas del Grupo Facebook han aportado a esta entidad.

Según Facebook Ireland Limited[55], *Cambridge Analytica* es una compañía que recibió información personal de usuarios de Facebook por parte de un desarrollador de aplicaciones, tercero ajeno a Facebook Inc., Dr. Aleksandr Kogan. Quien, afirma, transfirió información personal de los usuarios de Facebook obtenida a través de una aplicación que funcionaba con la plataforma Facebook[56]. Asimismo, Facebook Ireland Limited, como se dijo, precisó que setenta y cuatro (74) personas en Colombia instalaron la aplicación del Dr. Kogan, por medio de la cual se accedió a su información personal, y que aproximadamente fueron ciento cuarenta y seis mil seiscientas veintirés (146.623) personas en Colombia las afectadas por el acceso indebido a su información a través de dicha aplicación[57].

En la información aportada por Facebook Ireland Limited, a la presente actuación administrativa, se adjuntó un comunicado de Mark Zuckerberg (presidente, fundador y gerente de Facebook Inc.) de 21 de marzo de 2018, dirigido a los usuarios de Facebook, en el cual manifestó:

> "*Quiero compartir una actualización del caso de Cambridge Analytica (…) Nosotros tenemos una responsabilidad de proteger sus datos personales, y si no podemos entonces nosotros no los merecemos [a los usuarios de la Plataforma]. He estado trabajando para entender exactamente qué pasó y cómo puedo asegurar que esto no vuelva a pasar. Las buenas noticias es que las acciones más importantes para prevenir que esto pase de nuevo se han tomado ya desde hace años.* ***Pero hemos***

---

[54] 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.
[55] Folio 44
[56] Folio 45.
[57] Folio 46.

> ***cometido errores, es necesario hacer más, y necesitamos esforzarnos más y hacerlo.*** *(…)*
>
> *En 2013, un investigador de la Universidad de Cambridge llamado Aleksandr Kogan creó una aplicación sobre un quiz de personalidad. Esa aplicación fue instalada por cerca de 300.000 personas que compartieron su información personal, como también la de amigos de su perfil en la Plataforma.* ***Dada la forma en la que funcionaba la Plataforma en ese momento****,* ***significó que Kogan pudo acceder a la información personal de decenas de millones de los amigos de las personas que instalaron la aplicación****.*
>
> ***En 2014, para prevenir aplicaciones abusivas, anunciamos que cambiaríamos la Plataforma por completo para limitar de forma significativa la información a la cual pueden acceder las aplicaciones.*** *Más importante, aplicaciones como la de Kogan no podrían solicitar información acerca de los amigos de los usuarios que la instalaron a menos que esos amigos hayan autorizado la aplicación.*"[58] (énfasis añadido).

Como se observa, esta entidad no elucubró conclusiones en la Resolución 1321 de 2019, ni mucho menos fundamentó las órdenes en corrillos o invenciones. Las fuentes principales de la información que sustentaron dichas órdenes, provienen no solo de las mismas empresas del Grupo Facebook. Se trata de documentos con carácter declarativo y representativo, conforme con lo establecido el artículo 243 de la Ley 1564 de 2012 y al artículo 40 de la Ley 1437 de 2012.

De hecho, la misma recurrente en el escrito del recurso manifiesta que se enteró de que el Dr. Kogan posiblemente había compartido información personal de usuarios de la plataforma con *Cambridge Analytica*, al leer el periódico *The Guardian* en su publicación de 11 de diciembre de 2015[59]. Esa fue la primera fuente de información de Facebook Inc. para conocer que posiblemente se estaba accediendo de manera indebida, y violando sus Políticas de Privacidad, a los Datos personales de los usuarios.

Ninguna de las tres compañías vinculadas a este expediente tiene certeza sobre la información compartida por el Dr. Kogan y sus empresas. Según el recurso presentado, la información que Facebook Inc. tiene disponible, suministrada por el Dr. Kogan, permite afirmar que solo la información de usuarios ubicados en Estados Unidos fue accedida sin Autorización[60]. Sin embargo, se reitera que, esta autoridad mal haría en dar por cierta la información suministrada por el Dr. Kogan, quien según Facebook Inc. ni siquiera respetó sus Políticas de Privacidad. En razón a lo anterior, dar credibilidad a esa información no debería ser la primera opción de la recurrente ni de las demás empresas del Grupo Facebook. Si es que en realidad sí existe un interés real en conocer a ciencia cierta qué sucedió con la información obtenida y compartida por el Dr. Kogan.

Por otro lado, y sin necesidad de analizar todo su contenido, resulta imposible de ignorar la conclusión de la Investigación conjunta de Facebook, Inc. por el Comisionado de Privacidad de Canadá y el Comisionado de Información y Privacidad de Columbia Británica, en la que se afirmó que, Facebook no tenía garantías adecuadas para proteger la información personal de sus usuarios del acceso y uso no autorizados por parte de la aplicación TYDL, o con respecto a aplicaciones de terceros en general, en contra de las cláusulas 4.7 y 4.7.1 del anexo 1 de PIPEDA y la sección 34 de PIPA[61].

---

[58] Folios 58 y 470.
[59] Folio 500 (reverso).
[60] Folios 495 y 500.
[61] We find that Facebook did not have adequate safeguards to protect the personal information of its users from unauthorized access and use by the TYDL App, or in respect of third-party applications generally, contrary to clauses 4.7 and 4.7.1 of

Como señala la misma Resolución No. 1321 de 2019, la seguridad de la información personal "*no se limita [a] situaciones de infiltración o burla de las medidas de seguridad que ha implementado un Responsable o Encargado del Tratamiento."*[62]*;* según la Ley 1581 de 2012, en sus artículos 4 (literal g)[63]; 17 (literal c)[64]; y 18[65]. 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*"[66].**

De esta forma, las órdenes impuestas en la resolución recurrida, principalmente buscan reducir el riesgo de daño a su Derecho Fundamental a la Protección de Datos Personales. Esa función preventiva de las órdenes no es ajena a todas las medidas presentadas por Facebook Inc. en el recurso para proteger la privacidad y los Datos personales de los usuarios de Facebook.

La preocupación de esta entidad, como Autoridad de Protección de Datos Personales, es la misma de la recurrente en relación con la protección de los Datos personales de los usuarios y es la que llevó a solicitar en las órdenes impuestas una certificación de que las medidas que ha implementado Facebook Inc. son suficientes para garantizar esa protección y el cumplimiento del Régimen General de Protección de Datos Personales encabezado por el artículo 15 superior y la Ley 1581 de 2012.

Conforme con lo anterior, teniendo en cuenta la finalidad, el contenido y el objeto de la Resolución No. 1321 de 2019, esta entidad no considera necesario determinar con total certeza si son suficientes, o no, las medidas adoptadas hasta el momento por Facebook Inc. para proteger la privacidad de los usuarios de la Plataforma. Las órdenes impartidas buscan, de hecho, que Facebook Inc. acredite que las medidas implementadas, explicadas en detalle en el recurso presentado, son suficientes para proteger el Derecho Fundamental a la de *Habeas Data* de los usuarios y para cumplir con el Régimen General de Protección de Datos Personales. Razón por la cual, en el artículo segundo del acto recurrido, se exige una certificación emitida por una empresa con ciertas calidades, en la que se señale que todas las medidas adoptadas son suficientes y efectivas para los fines mencionados.

Así pues, es posible concluir que Facebook Inc. tiene tanta confianza en las medidas que ha adoptado, que dicha certificación no debe ser un obstáculo para el desarrollo de su actividad, sino la confirmación del deber cumplido.

En relación con este punto, la recurrente en el escrito bajo estudio manifestó que, su Programa de Privacidad es un marco integrado y completo con dos objetivos globales: i) abordar riesgos de privacidad relacionados con el desarrollo, la gestión y el uso de productos nuevos y existentes, y 2. Proteger la información que Facebook recibe de sus usuarios o aquella relacionada con los mismos. Asimismo, **afirma que su programa garantiza que los**

---

schedule 1 of PIPEDA and section 34 of PIPA. Recuperado de https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/ el 15 de marzo de 2020

[62] Folio 467 (reverso).

[63] "Artículo 4°. 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;(…)"

[64] "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; (…)"

[65] "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: (…) b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; (…)"

[66] Folio 467.

controles de privacidad funcionen adecuadamente, que las declaraciones de privacidad sean claras y precisas y que la compañía aborde proactivamente los riesgos emergentes en materia de privacidad. Razones que comparte esta autoridad, la cual impuso órdenes **preventivas** persiguiendo los mismos fines señalados por Facebook Inc.

Finalmente, al analizar nuevamente algunas líneas del escrito del recurso, *"(...) La SIC* [sic] *tampoco puede imponer medidas (incluso si se caracterizan como cautelares) para mitigar una situación que no se ha establecido como existente de hecho o por ley",* vale la pena decir que, si bien el comienzo de esa afirmación no es cierto, sí lo es que las medidas preventivas son precisamente para prever o disminuir la ocurrencia de determinada situación. De ahí el carácter previsible de las órdenes impuestas.

8. CIBERSEGURIDAD

Una empresa tan determinante en la ciberseguridad del mundo como lo es Facebook, en razón de la cantidad y calidad de información que maneja, tiene el deber de ser más que diligente en el Tratamiento de Datos, a fin de garantizar la protección de las personas y su privacidad. Por eso, esa empresa no debería ahorrar esfuerzos para mejorar los niveles de seguridad que exige la regulación para todos los usuarios de esa red social digital.

Como es sabido, la regulación de la República de Colombia no solo ordena a quien trate Datos personales a implementar 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*"[67] y a "*conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"* [68]. Sino que, se reitera, les exige "*(…) 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"*[69].

No debe perderse de vista que, Facebook es la red social digital con mayor número de usuarios en el mundo y en la República de Colombia. Pues, en efecto, cuenta con aproximadamente dos mil cuatrocientos veintiséis (2.426) millones de usuarios[70] en todo el mundo. En cuanto a Colombia, la cifra de usuarios es de treinta y uno (31) millones de personas. Es decir, el 68% de los colombianos utiliza esa plataforma.

En el escrito del recurso, Facebook Inc. argumenta que, *"(...) Los usuarios se han unido a Facebook en cifras* ***muy significativas*** *precisamente porque desean participar en la cultura del intercambio, la cual es la base de la experiencia de Facebook y para disfrutar de las experiencias en línea sociales personalizadas que ofrece Facebook (...)".* (Destacamos). Así es que, con mayor razón se exige un nivel de conservación superior de la seguridad informática, apartado de la simple excusa de ser un *"intermediario"* entre los usuarios.

Por eso, 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**.

Se reitera que, la orden impartida es de carácter **preventivo,** para evitar que se afecte la seguridad de los Datos de los colombianos. La misma se adoptó teniendo en cuenta, entre

---

[67] Cfr. Literal g) del artículo 4 de la Ley Estatutaria 1581 de 2012
[68] Cfr. Literal d) del artículo 17 de la Ley Estatutaria 1581 de 2012
[69] Cfr. Artículo 26 del decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015)
[70] Cfr. Internet Live Stacts https://www.internetlivestats.com/ (Última consulta: 13 de febrero de 2020)

otros, los hechos; investigaciones; actuaciones y conclusiones 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 de Norteamérica) que tienen como objetivo 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 *(particularmente el escándalo de Cambridge Analítica)* no ocurra nuevamente.

Teniendo en cuenta 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*, esta entidad considera que la orden es necesaria y su cumplimiento imperativo por parte de Facebook para garantizar en la práctica, la seguridad de los Datos personales y de los ciudadanos usuarios de esa red social digital.

Sin seguridad no hay debido Tratamiento de Datos personales. Así las cosas, Facebook debe ser responsable, diligente y muy profesional con el Tratamiento seguro de los mismos.

9. EN EL "CIBERESPACIO" NO DESAPARECEN LOS DERECHOS DE LAS PERSONAS: MENSAJE DE LA CORTE CONSTITUCIONAL

La realidad socio tecnológica del Siglo XXI no pone de presente la migración del mundo físico y fronterizo al "ciberespacio", el cual se caracteriza por ser tecnológico y sin fronteras geográficas.

Existen diversas referencias sobre lo que significa el ciberespacio. El 8 de febrero de 1996, por ejemplo, se hizo pública la Declaración de Independencia del Ciberespacio[71] en la cual se utilizaron expresiones como "el nuevo hogar de la mente" y un "espacio social global" en construcción para referirse al mismo. Allí, también se señaló que el ciberespacio no está dentro de las fronteras de los actuales gobiernos, ya que es un mundo inmaterial que "está a la vez en todas partes y en ninguna parte".

Posteriormente, en el Diccionario de la Real Academia de la Lengua Española se incluyó la palabra "ciberespacio" para hacer referencia a un *"ámbito artificial creado por medios informáticos"*. Destacamos de lo anterior, la connotación inmaterial y artificial que desde un principio se ha asociado al ciberespacio para contrastarlo con las actividades materiales y reales que acontecen en el mundo territorial y, especialmente, en Internet.

Para el Profesor Lessig, el ciberspacio hace alusión a una "nueva sociedad" que surgió en los países occidentales en la "mitad de la década de los años noventa". En un principio en "las universidades y centros de investigación", y luego en la sociedad en general. Internet es esa nueva sociedad a la que se refiere dicho autor, la cual gira en torno a una *"estructura abierta y de finalidad múltiple de las redes basadas en la transferencia de paquetes de datos (…) en la que cada persona podría ejercer como su propio redactor-jefe y publicar lo que desease"*[72].

---

[71] Esta declaración es un texto presentado por John Perry Barlow en Davos (Suiza), confundador de la Electronic Frontier Foundation (https://www.eff.org/). No se trata de un instrumento jurídico vinculante sino de un manifiesto que buscaba que los gobiernos no interfirieran en lo que sucede en internet. El texto puede consultarse en: https://projects.eff.org/~barlow/Declaration-Final.html Última consulta: octubre 20 de 2014)
El texto es una reivindicación que critica las interferencias de los poderes políticos que afectan al mundo de Internet y defiende la idea de un ciberespacio soberano.

[72] Las expresiones y frases entre comillas son tomadas de: LESSIG, Lawrence. 2001. El código y otras leyes del ciberespacio. Traducción de E. Alberola, Colección taurusesdigital. Madrid, España: Grupo Santillana de Ediciones S.A. p. 21). Este mismo autor previamente analizó otros aspectos sobre el ciberespacio en: LESSIG, Lawrence. 1996. The zones of cyberspace. Stanford Law Review 48:1403-1411.

En el caso de la regulación colombiana[73], la Comisión de Regulación de Comunicaciones incorporó la siguiente definición en el numeral 9 del artículo 1 de la Resolución No. 2258[74] de 23 de diciembre de 2009: "*Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios*".

En la exposición de motivos de dicha norma se destaca que, "*la protección del ciberespacio es un factor de trascendente importancia para preservar la seguridad de la Nación y su economía, y que para avanzar en este objetivo, se requiere de un marco regulatorio que asegure la protección de los aspectos vulnerables de la infraestructura de la información que se adapte a las necesidades del entorno. En tal sentido, los estudios desarrollados por la CRC recomiendan adoptar medidas complementarias a las dispuestas en las Resoluciones CRT 1732 y 1740 de 2007, con el propósito de establecer condiciones asociadas a la inviolabilidad de las comunicaciones y la seguridad de los datos e informaciones, garantizar la seguridad de la red así como la integridad de los servicios*."

La definición y los considerandos constatan que el ciberespacio está llamando la atención de los reguladores a pesar que se trata de un escenario electrónico o "virtual". Lo relevante del tema es no perder de vista que en el ciberespacio interactúan personas reales de diferente nacionalidad y domiciliadas en prácticamente cualquier parte de nuestro planeta cuyas comunicaciones y actividades traspasan el espacio geográfico de todos los países del mundo.

Aunque existen diferentes acepciones sobre el ciberespacio, consideramos relevante tener presente que el mismo está integrado por los siguientes elementos[75]:

i. Una infraestructura tecnológica (recursos tecnológicos) conformada por un sinnúmero de equipos (servidores, computadores, teléfonos móviles, tabletas, entre otras) que se encuentran ubicados en muchas partes del mundo.

ii. Una plataforma de comunicaciones (red global de comunicaciones), información y redes interconectadas (Internet) de alcance mundial denominada *"infraestructura global de información"*[76].

iii. Millones de personas de diversas nacionalidades, domiciliadas en países con sistemas jurídicos disímiles que desde cualquier parte hacen uso de la tecnología, las comunicaciones y la información para interactuar con otras personas o utilizar los servicios disponibles en Internet.

El ciberespacio ha sido caracterizado por ser un escenario global no delimitado por fronteras geográficas[77] en donde las actividades suceden dentro de la arquitectura tecnológica de Internet. Acá no existe un espacio físico definido (como nuestra casa o el territorio de nuestro país) sino un campo artificial o virtual e indeterminado en donde las personas interactúan. Buena parte de esas actuaciones en el mundo virtual tienen implicaciones y consecuencias jurídicas en el mundo real.

---

[73] La literatura colombiana se ha referido al ciberespacio pero desde la perspectiva de la seguridad y los conflictos armados. En este sentido, consultar el siguiente libro: GAITÁN RODRIGUEZ, Andrés. 2012. El ciberespacio. un nuevo teatro de batalla para los conflictos armados del siglo XXI. Bogotá, Colombia: Escuela Superior de Guerra.

[74] Por la cual se modifican los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1.8 y 2.4 de la Resolución CRT 1740 de 2007

[75] Sobre algunas características del ciberespacio y los retos que genera al Derecho véase: JOHNSON, David y POST, David. 1995-1996. Law and borders: the rise of law in cyberspace. Stanford Law Review 48:1367-1402.

[76] Reidenberg se refiere a ella como "the global information infrastructure –GII-" (REIDENBERG, Joel R. 1996. Governing networks and cyberspace rule-making. Emory Law Journal 45. p 912)

[77] Cfr. GILDEN, Michael. 2000. Jurisdiction and the internet: the real world meets cyberspace. ILSA Journal of International & Comparative Law 7 (1). P 150

En suma, el ciberespacio hace alusión a un ámbito imaginario, intangible e invisible - en contraposición al mundo real y físico- en donde tienen lugar una serie de acontecimientos que suceden en Internet. Y, aunque se trata de un "mundo virtual", sus ciudadanos son miles de millones de personas reales ubicadas en prácticamente cualquier lugar del "mundo físico" cuyas actividades tienen impacto o consecuencias en el "mundo real"[78].

Ahora bien, en 2001 la Corte Constitucional de la República de Colombia se pronunció sobre, entre otros, el alcance del ordenamiento constitucional frente a la regulación de materias ligadas al ejercicio de actividades a través de Internet [79]. Para la Corte, la información es muy importante y cumple un rol central "en el funcionamiento de la sociedad actual" e Internet ha sido, entre otros, un escenario en el cual operan muchos "sistemas de información y almacenamiento informático".

De entrada, la Corte rápidamente advierte sobre lo que sucede con la información que es recolectada en el "mundo virtual" –ciberespacio-. En este sentido, manifiesta que, "la información que se comparte en Internet deja una huella que, por ejemplo, no solo permite establecer el contenido exacto de la transacción comercial efectuada entre un usuario del sistema y el agente material de una actividad que se desarrolla por esta vía (…) sino que, hace posible rastrear e identificar todo lo que una persona hizo en el **mundo virtual**, los lugares que visitó o consultó y los productos que consumió a través de la red. **La recopilación de estos Datos puede ser utilizada para crear perfiles** sobre los gustos, preferencias, hábitos de consulta y consumo de las personas que emplean Internet (como simples usuarios o como agentes económicos que desarrollan sus actividades por este medio)." [80] (Negrilla ausente en el original).

De otra parte, la Corte también reconoció la importancia "que tienen dentro de un sistema global de comunicaciones, como Internet, derechos y libertades tan importantes para la democracia como (…) la intimidad y el *habeas data* (artículo 15 C.P.)"[81]Adicionalmente, dicha corporación admitió que los avances científicos y tecnológicos "**siempre han planteado retos al derecho**" porque éstos inciden, entre otros, "en el ejercicio de los derechos fundamentales de las personas" y por ende "**demandan diferentes respuestas del ordenamiento jurídico**"[82]. (Énfasis añadido).

A pesar que el campo de acción de Internet desborda las fronteras nacionales, para la Corte Constitucional el nuevo escenario tecnológico y las actividades en Internet no se sustraen del respeto de los mandatos constitucionales[83]. Por eso, concluye dicha entidad 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**" [84]. (Negrilla ausente en el original),

---

[78] De hecho, autores como Baronti, han afirmado que el ciberespacio es en últimas una "una proyección simbólica del mundo real" (Cfr. BARONTI, Hugo. 2014. ¿Qué es el ciberespacio?. En: http://baronti.net/textos/292-¿que-es-el-ciberespacio.html (última consulta: octubre 22 de 2014)

[79] Cfr. Corte Constitucional. Sentencia C-1147 del 31 de octubre de 2001. MP. Dr. Manuel José Cepeda Espinosa.

[80] Todas las partes o frases señaladas entre comillas son tomadas de la Sentencia C-1147 de 2001

[81] Los otros derechos importantes que cita el alto tribunal son: el derecho a la igualdad ; la libertad de conciencia o de cultos; la libertad de expresión; el libre ejercicio de una profesión u oficio; el secreto profesional y el ejercicio de los derechos políticos que permiten a los particulares participar en las decisiones que los afectan (Corte Constitucional, C-1147 de 2001)

[82] Todas las partes o frases señaladas entre comillas son tomadas de la Sentencia C-1147 de 2001

[83] En efecto, subraya la Corte Constitucional que "los mandatos expresados en la Carta Política cobran un significado sustancial que demanda del juez constitucional la protección de los derechos reconocidos a todas las personas, pues se trata de garantías que también resultan aplicables en ese ámbito" (Corte Constitucional, C-1147 de 2001)

[84] Todas las partes o frases señaladas entre comillas son tomadas de la Sentencia C-1147 de 2001

CONCLUSIONES

Sin perjuicio de lo establecido, no se accederá a las pretensiones de Facebook Inc. Por las siguientes razones:

1. La Ley Estatutaria 1581 de 2012 es aplicable a Facebook Inc. porque dicha empresa recolecta Datos personales en el territorio de la República de Colombia a través de *cookies* que instala en los equipos o dispositivos de las personas residentes o domiciliadas en Colombia;
2. La Ley Estatutaria 1581 de 2012 es aplicable, entre otras, cuando: i) El Tratamiento lo realiza el Responsable o Encargado, domiciliados o no en territorio colombiano, que directa o indirectamente, a través de cualquier medio o procedimiento, físico o electrónico, recolecta, usa, almacena o trata Datos personales en el territorio de la República de Colombia; y ii) El Responsable o Encargado no está domiciliado en la República de Colombia ni realiza Tratamiento de Datos dentro del territorio colombiano. Pero, existen normas o tratados internacionales que los obliga a cumplir la regulación colombiana;
3. Aunque Facebook Inc. no está domiciliado físicamente en Colombia, utiliza herramientas electrónicas dentro del territorio de nuestro país para recolectar Datos personales. Por ende, Facebook Inc. realiza Tratamiento de Datos personales en territorio colombiano al cual le es aplicable la Ley Estatutaria 1581 de 2012;
4. Facebook Inc. es Responsable del Tratamiento de los Datos personales que recolecta en el territorio colombiano a través de *cookies*. Así las cosas, Facebook Inc. debe cumplir la Ley Estatutaria 1581 de 2012 y sus disposiciones reglamentarias;
5. El Principio de Responsabilidad Demostrada (*Accountability)* frente al Tratamiento de Datos personales, le impone a Facebook Inc. el deber de probar que ha adoptado medidas apropiadas y efectivas para garantizar la seguridad de la información de sus usuarios;
6. Una orden administrativa no es una sanción, sino una medida preventiva para que, entre otras, se garantice la seguridad en el Tratamiento de los Datos personales de los usuarios de Facebook. Las sanciones por infringir la Ley Estatutaria 1581 de 2012 *-multas, suspensión de actividades, cierre temporal o definitivo-* están previstas en el artículo 23 de dicha norma. Allí se puede constatar que las órdenes no son sanciones;
7. Esta superintendencia sí tiene competencia para imponer las órdenes contenidas en la Resolución No. 1321 de 2019 tal y como se puede evidenciar en el literal e) del artículo 21 de la Ley Estatutaria 1581 de 2012;
8. En el desarrollo de la actuación administrativa que terminó con la expedición de la Resolución No. 1321 de 2019 se respetaron todas las garantías procesales, constitucionales y legales, y los Derechos Fundamentales de la recurrente;
9. El procedimiento seguido para emitir la Resolución No. 1321 de 2019 es el previsto en la ley para este tipo de actuaciones;
10. Facebook Inc., Facebook Colombia S.A.S. y Facebook Ireland Limited, de conformidad con lo establecido en el artículo 4 de la Constitución Política Nacional, tienen la obligación de cumplir las órdenes impartidas en la Resolución No. 1321 de 2019;
11. Una empresa tan determinante en la ciberseguridad del mundo como lo es Facebook, en razón de la cantidad y calidad de información que maneja, tiene el deber de ser más que diligente en el Tratamiento de Datos, a fin de garantizar la protección de las personas y su privacidad. Por eso, esa empresa no debería ahorrar esfuerzos para mejorar los niveles de seguridad que exige la regulación para todos los usuarios de esa red social digital.

Sin seguridad no hay debido Tratamiento de Datos personales. Así las cosas, Facebook debe ser responsable, diligente y muy profesional con el Tratamiento seguro de los Datos de sus usuarios.

En mérito de lo expuesto, este Despacho,

RESUELVE

PRIMERO. Confirmar en todas sus partes la Resolución No. 1321 de 24 de enero de 2019, por las razones expuestas en la parte motiva de este acto administrativo.

SEGUNDO. Notificar personalmente el contenido de la presente resolución a la sociedad a **Facebook Inc.,** a través de los medios autorizados por el Decreto 491 del 28 de marzo de 2020 y de la forma indicada en su artículo 4, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

TERCERO: Informar el contenido de la presente resolución al Director de Investigación de Protección de Datos Personales y devolverle el expediente para su custodia final.

NOTIFÍQUESE Y CÚMPLASE
Dada en Bogotá, D.C., 01 de Abril de 2020

El Superintendente Delegado para la Protección de Datos Personales,

NELSON REMOLINA ANGARITA

CGC

Notificación

Sociedad: Facebook Inc.
Representante legal: [redacted]
Identificación: [redacted]
Dirección 1: [redacted]
Dirección 2: [redacted]
Estado: California
Código Postal: [redacted]
País: Estados Unidos de Norteamérica
Dirección electrónica 1: [redacted]