



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

RESOLUCIÓN NÚMERO 59876 DE 2020

(28 de Septiembre)

Radicación 19-40311

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. 21478 de 17 de junio de 2019, la Dirección de Investigación de Protección de Datos Personales resolvió:

**“ARTÍCULO PRIMERO: ORDENAR** a las sociedades **UBER TECHNOLOGIES, INC., UBER COLOMBIA SAS** [sic] y **UBER B.V.**, en adelante **UBER**, implementar medidas y procedimientos para la adecuación de sus operaciones en la República de Colombia a las disposiciones de la Ley 1581 de 2012, las cuales deberán contener como mínimo los siguientes estándares:

1. Mejorar o robustecer las medidas de seguridad que ha implementado a la fecha de expedición de la presente resolución para garantizar la seguridad de los datos [sic] personales, evitando su: (i) acceso no autorizado o fraudulento; (ii) uso no autorizado o fraudulento; (iii) consulta no autorizada o fraudulenta; (iv) adulteración o (v) pérdida.

2. Desarrollar, implementar y mantener un programa integral de seguridad de la información, que garantice la seguridad, confidencialidad e integridad 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 e indicadores de cumplimiento y tener en cuenta, como mínimo, lo siguiente:

- a) Los principios rectores establecidos en la Ley 1581 de 2012 y los deberes que de ellos se derivan;
- b) El tamaño y la complejidad de las operaciones de UBER;
- c) La naturaleza y el ámbito de las actividades de UBER;
- d) La cantidad de titulares [sic];
- e) La naturaleza de los datos [sic] personales;
- f) El tipo de Tratamiento de los datos [sic] personales;
- g) El alcance, contexto o fines del Tratamiento;
- h) Las actualizaciones o cualquier tipo de modificación en las Aplicaciones [sic] de UBER, sus productos y cualquier otra forma en que UBER utilice, recopile, o comparte los datos [sic] recogidos;
- i) El acceso a los datos [sic] personales por parte de los empleados o contratistas de UBER;
- j) El uso de los datos [sic] personales de los usuarios por terceros, entre ellos, aliados comerciales, empresas asociadas y desarrolladores de Aplicaciones [sic], si aplica;

*Por la cual se resuelve un recurso de apelación*

- k) El uso innovador o aplicación de nuevas soluciones tecnológicas;*
- l) Los riesgos internos y externos para la seguridad, confidencialidad y disponibilidad de los datos [sic] personales; y,*
- m) Los riesgos para los derechos y libertades de las personas.*

*3. Desarrollar, implementar y mantener un programa de gestión y manejo de incidentes 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 de los mismos cuando se presenten incidentes que afecten la confidencialidad, integridad y disponibilidad de los datos [sic] personales.*

*4. Desarrollar, implementar y mantener un programa de capacitación y entrenamiento rutinario para sus empleados y contratistas sobre su política de seguridad de la información, su política de gestión de incidentes de seguridad de datos [sic] personales y su política de tratamiento [sic] de datos [sic] personales (o privacidad) de UBER.*

*5. Poner en marcha un sistema de monitoreo permanente para verificar si, en la práctica, sus medidas de seguridad son útiles, suficientes o si están funcionando correctamente. En caso [sic] que ello no sea así, adoptar las medidas necesarias para garantizar la seguridad de la información.*

*6. UBER 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:** *Las sociedades **UBER TECHNOLOGIES, INC., UBER COLOMBIA SAS** [sic] y **UBER B.V.** deberán cumplir lo ordenado en esta resolución dentro de los **CUATRO (4)** meses siguientes a la ejecutoria del presente acto administrativo y acreditar ante esta Superintendencia [sic] las medidas y procedimiento adoptados dentro de los **CINCO (5)** días siguientes al vencimiento de dicho término.*

**PARÁGRAFO PRIMERO:** *Para demostrar el cumplimiento deberán remitir, al finalizar dicho plazo, una certificación emitida por una entidad o empresa, nacional o extranjera, independiente, imparcial, profesional y especializada 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.*

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

**PARÁGRAFO TERCERO:** *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*

*Por la cual se resuelve un recurso de apelación*

*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 UBER COLOMBIA S.A.S. que preste su colaboración para que UBER TECHNOLOGIES, INC., y UBER B.V. cumplan las instrucciones y órdenes impartidas por esta Superintendencia [sic] en esta resolución (...)*

**SEGUNDO.** Que, por medio de comunicación 19-40311-12<sup>1</sup> de 17 de julio de 2019, **UBER COLOMBIA S.A.S.** presentó recurso de reposición y, en subsidio apelación en contra de la Resolución No. 21478 de 17 de junio de 2019, en el cual argumentó lo siguiente:

#### **ANOTACIÓN PRELIMINAR**

*“(...) la SIC (...) llega al extremo de considerar que es necesario impartirle órdenes preventivas a “UBER”, siendo que la propia Resolución [sic] Impugnada [sic] se refiere a “UBER” como unas aplicaciones y no como unas sociedades.*

*(...) ello redunda en una muy grave violación del derecho de defensa y audiencia no sólo [sic] de la Compañía [sic] sino de las otras dos sociedades también referidas en la [Resolución [sic] Impugnada [sic], quienes ahora tienen la carga de defenderse respecto de unas manifestaciones e imputaciones que, por una parte, y según la propia Resolución [sic] Impugnada [sic], se predicen es de unas aplicaciones y no de unas compañías. Y que, por la otra, no distinguen entre cada una de esas sociedades, sus objetos sociales, las actividades a las que se dedican, y, sobre todo, su eventual rol frente a los datos [sic] personales en los términos de la ley .*

*(...) todo parece indicar que, deliberadamente, la SIC optó por no entrar a diferenciar entre Uber Technologies, Inc., Uber B.V. y la Compañía [sic], como ha debido hacerlo- para (...) impartir órdenes a las tres compañías (...) sin analizar cuál es el objeto social de cada sociedad y cuál podría ser su responsabilidad en relación con los datos [sic] personales que son tratados a través de las aplicaciones “UBER”.*

#### **CUESTIÓN FUNDAMENTAL**

*Esta circunstancia (...) es manifiestamente contraria a la ley, y, sobre todo, a los derechos fundamentales de las tres sociedades objeto de las órdenes (...).*

- 1. “(...) la Compañía [sic] no es propietaria, arrendataria, licenciataria , beneficiaria ni bajo ningún contexto o razón usuaria, administradora y/o responsable de la aplicación UBER. Así pues, como en su momento lo reconoció la Superintendencia [sic] de Transporte, mi representada no maneja, manipula, controla ni mucho menos administra una plataforma o aplicación informática (...).*

*(...) la Compañía [sic] tiene acceso a información limitada sobre usuarios-pasajeros y usuarios-conductores registrados en la aplicación y/o plataforma tecnológica “UBER”, aprovechable desde Colombia. El rol de mi representada con relación a algunos datos [sic] que se tratan a través de la aplicación y/o plataforma tecnológica “UBER”, en*

<sup>1</sup> De conformidad con la certificación de 28 de agosto de 2019, expedida por la Secretaria General Ad.-Hoc (Coordinadora del Grupo de Notificaciones y Certificaciones) de la Superintendencia de Industria y Comercio, la Resolución No. 21478 de 17 de junio de 2019 fue notificada por conducta concluyente a UBER COLOMBIA S.A.S., el 17 de julio de 2019. Con lo cual, el término para presentar los recursos vencía el 31 de julio de 2019. Así las cosas, los recursos se presentaron en la oportunidad procesal correspondiente.

*Por la cual se resuelve un recurso de apelación*

*Colombia, es el de Encargado del Tratamiento, obrando frente a los mandatos recibidos por parte de Uber BV. Dicho tratamiento [sic], hecho por cuenta del Responsable del Tratamiento, implica en sí mismo que mi representada no decide sobre la base [sic] de datos [sic] ni sobre el tratamiento [sic] hecho sobre dichas categorías limitadas de datos (...).*

*Mi representada (...) no detenta la condición de responsable [sic] sobre las base [sic] de datos [sic] usuarios-pasajeros y de usuarios-conductores de la aplicación y/o plataforma tecnológica UBER. (...) por cuanto no decide: (i) sobre el uso dado a esta información; (ii) sobre las finalidades del tratamiento la base [sic] de datos [sic]; (iii) los medios utilizados para alcanzar dichas finalidades; (iv) ni mucho menos es la persona que se identifica como “responsable” [sic], en la Política de Tratamiento de la Información correspondiente.*

*(...) la Compañía [sic] cumple un rol limitado como encargado [sic] del tratamiento [sic] frente a algunas categorías de datos [sic], por expreso mandato de UBER BV, a través de la aplicación UBER, motivo por el cual de ninguna manera puede predicarse que, en dichos tratamientos [sic], actúa como Responsable (...).*

#### **MOTIVOS DE INCONFORMIDAD CON LA RESOLUCIÓN IMPUGNADA Y QUE EVIDENCIAN QUE LA MISMA DEBERÁ SER REVOCADA**

##### **A. Falta de competencia de la Delegatura para la Protección de Datos Personales para impartir las órdenes contenidas en la Resolución [sic] Impugnada [sic] a la Compañía**

*(...) no puede la SIC impartirle órdenes a un Encargado como si fuera un Responsable, y viceversa, pues ello redundaría en un evidente ejercicio indebido de la facultad conferida por el literal e) del artículo 21 de la Ley 1581 de 2012, es decir, en una actuación por fuera de los linderos trazados por el legislador para dictar este tipo de órdenes .*

*(...) la Resolución [sic] Impugnada [sic] simplemente optó por impartirle órdenes a las tres compañías, indistintamente y por igual, como si todas esas sociedades, incluida mi representada, tuvieran la calidad de Responsables (...).*

*(...) la Compañía no es Responsable del Tratamiento con relación a la información recolectada en las aplicaciones y plataforma tecnológicas de UBER, pues esta responsabilidad le corresponde única y exclusivamente a Uber B.V., circunstancia que, inclusive, también fue expresamente reconocida por la SIC mediante Resolución No. 88509 de 2018.*

*(...) la SIC ha debido analizar cuál es el objeto social de cada sociedad objeto de las órdenes u [sic] medidas, y cuál podría ser su responsabilidad en relación con los datos [sic] personales que son tratados a través de las aplicaciones “UBER”. Porque de haberlo hecho, hubiera concluido, como ya lo hizo en diciembre de 2018, que mi representada no es Responsable del Tratamiento de los datos [sic] personales recolectados por la aplicación UBER.*

*(...) esta Dirección carece de competencia para impartirle a mi representada las órdenes contempladas en la Resolución [sic] Impugnada [sic], pues como es claro ya,*

*Por la cual se resuelve un recurso de apelación*

*dichas órdenes solamente pueden impartirse a quien ostenta la calidad de Responsable (...).*

**B. *Violación al derecho [sic] fundamental [sic] al debido [sic] proceso [sic] y a la defensa de la Compañía [sic]***

*1. La Resolución [sic] Impugnada [sic] desconoció la presunción de inocencia (...)*  
*(...)*

*Esto se confirmó con el hecho mismo de que se expidiera la Resolución [sic] Impugnada [sic] sin que siquiera se surtiera un procedimiento administrativo encaminado a verificar si jurídicamente era posible impartirle semejantes órdenes a mi representada.*

*(...) la SIC expidió la Resolución [sic] Impugnada [sic] adaptando a su conveniencia las competencias y funciones que le otorga la ley, realizando conjeturas con los documentos recopilados sin que se logre probar la necesidad de lo ordenado más allá de la duda razonable, y presumiendo la culpabilidad de mi representada bajo el entendido de que ni siquiera merecía algún tipo de audiencia previo a adoptar las órdenes y medidas objeto de dicho acto administrativo.*

*2. La Resolución [sic] Impugnada [sic] viola la garantía del non bis in ídem [sic]*

*(...) mediante la Resolución No. 88509 de 5 de diciembre de 2018, la Dirección de Investigaciones de Protección de Datos Personales inició una investigación administrativa y formuló cargos en relación con “los datos [sic] recolectados por la aplicación ‘UBER’”*

*Esta investigación todavía se encuentra en curso. De hecho, mediante la Resolución No. 20209 de 10 de junio de 2019 esta Dirección decretó la práctica de unas pruebas dentro del recurso de reposición, y en subsidio de apelación, interpuesto por la Compañía [sic] contra el numeral tercero de la parte resolutive de la Resolución No. 88509.*

*(...) el respeto de la garantía del non bis in ídem [sic] le imponía a la SIC la obligación de no iniciar ni adelantar ningún procedimiento administrativo adicional sobre los mismos hechos (...) en la Resolución [sic] Impugnada [sic], el Despacho hace juicios de valor negativos sobre las compañías a las que se refiere, y les impone -de manera indistinta- cargas como resultado de unas supuestas infracciones, situaciones propias del marco administrativo sancionatorio.*

*La sola existencia de este trámite administrativo implica una muy grave violación al principio constitucional en comento (...)*

*3. No existió ningún material probatorio idóneo en que se pudiera fundar la Resolución [sic]*

*(...) la Resolución [sic] Impugnada [sic] se expidió sin ninguna prueba que: (i) justificara las órdenes y medidas contempladas en la misma; y (ii) hubiera podido haber sido controvertida por mi representada.*

*Lo único que reposa en el expediente son unas comunicaciones y una correspondencia, la cual ni por asomo da cuenta de lo que se menciona en la*

*Por la cual se resuelve un recurso de apelación*

*Resolución [sic] Impugnada [sic], ni mucho menos legitima la adopción de las decisiones contenidas en dicho acto administrativo.*

*(...) la Resolución [sic] Impugnada [sic] enlista toda una serie de supuestas órdenes y sanciones proferidos por autoridades extranjeras. Y, sin embargo, ninguna de esas órdenes y sanciones se refiere y/o relaciona con la Compañía, ni le son oponibles.*

*(...) todas esas órdenes y medidas se refieren al mismo incidente ocurrido en el año 2016, en relación con el cual la Compañía no tuvo ninguna relación ni control. ¿Acaso qué lecciones puede derivar o aprender mi representada de una serie de órdenes y medidas que no la involucran y que no tienen ninguna relación con ella?*

*(...) todas esas supuestas órdenes y medidas de autoridades extranjeras se encuentran en idiomas distintos del castellano. De hecho, no hay una sola de esas órdenes y medidas que hubiera sido dictada en este idioma. Por ende, para poderlas incorporar en el expediente, y, más aún, para fundamentar en ellas la expedición de la Resolución [sic] Impugnada [sic], la Superintendencia [sic] ha debido proceder con la traducción oficial de esas órdenes y medidas, tal como lo ordena el artículo 251 del Código General del Proceso (...).*

*(...) no puede pasarse por alto (...) que esas aludidas órdenes y medidas de autoridades foráneas fueron obtenidas a partir de unas consultas en internet por funcionarios de la SIC, sin la audiencia o participación de ninguna de las sociedades objeto de este acto administrativo y, sobre todo, sin que respecto de esas supuestas pruebas ninguna sociedad haya podido pronunciarse ni formular reparo, comentario u objeción alguna. Es decir, mi representada no tuvo la oportunidad de ejercer su derecho de contradicción de la prueba.*

*(...)*

- 4. La Resolución [sic] Impugnada [sic] contrarió el principio de legalidad y vulneró el derecho a la defensa de la Compañía al haber omitido adelantar un procedimiento administrativo en el que se discutiera y probaran los hechos y circunstancias en que se basó la Superintendencia para expedirla.*

*La garantía del debido procedimiento sancionatorio indica que la imposición de cualquier medida o sanción debe estar precedida de un procedimiento administrativo que determine la necesidad de reprochar una contravención legal por parte de un particular.*

*(...) la SIC, previo a impartir las órdenes contenidas en la Resolución [sic] Impugnada [sic], estaba por ley sujeta a adelantar averiguaciones preliminares, de ser el caso, formular cargos, frente a los cuales los administrados tienen derecho de presentar los correspondientes descargos y solicitar el decreto y práctica de pruebas, surtir el periodo probatorio, correr traslado para alegar de conclusión y una vez efectuado todo el trámite de ley, proceder a adoptar la decisión correspondiente.*

*Así, conforme a la ley, y sin perjuicio de que no era posible adelantar un segundo trámite por cuenta del principio non bis in ídem, la Resolución [sic] es una decisión que debía estar precedida de un procedimiento administrativo sancionatorio, toda vez que la naturaleza de la orden impartida no solamente implica la modificación*

Por la cual se resuelve un recurso de apelación

de una situación jurídica para los sujetos de la misma, sino que, además le representa unos gastos y sobrecostos sumamente altos que no se encuentran en la obligación de asumir.

(...) la SIC negó a mi representada las garantías mínimas del debido proceso, puesto que no le permitió el ejercicio de su defensa. Es decir, en el curso de la actuación dentro de la cual se dictó el acto administrativo, no la oyó ni le permitió presentar argumentos y/o pruebas tendientes a desvirtuar las acusaciones e imputaciones que hizo en su contra, ni presentar los alegatos correspondientes.

Y, lo que es peor, la SIC ni siquiera se preocupó por justificar las razones por las cuales considera que en este caso se puede prescindir del ejercicio del derecho de defensa, y aun así, emitir órdenes en contra de mi representada, a todas luces improcedentes y desproporcionadas.

(...) contrario a lo que el respeto mínimo por el debido proceso indica, la SIC no se tomó el trabajo de concluir ningún tipo de procedimiento administrativo para llegar a un convencimiento sobre la necesidad de proferir la Resolución [sic] Impugnada [sic] (...).

### C. Falsa Motivación de la Resolución [sic] Impugnada [sic]

(...) la SIC consideró que había lugar a impartirle a mi representada las órdenes y medidas contempladas en la Resolución [sic] Impugnada [sic], con base en tres premisas, a saber:

i. En el numeral 19.1.8 señala la Superintendencia [sic] que:

19.1.8. Se concluye, en este punto, que UBER TECHNOLOGIES, INC., UBER B.V. y UBER COLOMBIA SAS son tres agentes o compañías que hacen parte del grupo "UBER", que, en virtud del reparto de funciones dentro del grupo, intervienen conjuntamente en el desarrollo, la distribución y la explotación de los servicios de "UBER", incluida las aplicaciones que están disponibles en territorio colombiano, descargadas a través de dispositivos móviles dentro del territorio colombiano y usadas por personas domiciliadas o residentes en el territorio colombiano para los fines señalados en la política de privacidad de "UBER".



ii. Seguidamente, en el numeral 19.2.5 manifiesta la Resolución Impugnada que la Compañía recolecta datos personales "para prestarle a 'UBER' 'servicios de mercadeo y publicidad, y servicios operacionales y de soportes de clientes'".

iii. Y, finalmente, en el numeral 19.2.6 se lee lo siguiente:

"19.2.6. Además, por su intervención en el desarrollo, la distribución y la explicación de los servicios y productos bajo la marca 'UBER', les corresponden a UBER TECHNOLOGIES, INC., UBER COLOMBIA S.A.S. y UBER B.V., por sí mismos o conjuntamente, la responsabilidad de velar por el cumplimiento de todos los requisitos establecidos en la Ley 1581 de 2012."

Página 18 del recurso presentado

(...) como en su momento lo reconoció la Superintendencia de Transporte, y se concluye de la decisión de la propia SIC con Rad. No. 18-178075—12, del [sic] 10 de diciembre de 2018, mi representada no maneja, manipula, controla ni mucho menos administra una plataforma o aplicación informática (...), las actividades a las que se dedica la compañía están expresa y debidamente enlistadas en su objeto social.

Por la cual se resuelve un recurso de apelación

(...) aún [sic] si en gracia de discusión fuera cierto lo que dice la Resolución [sic] Impugnada [sic] respecto de a que mi representada supuestamente interviene “en el desarrollo, la distribución y la explotación de los servicios de UBER”, ello tampoco justificaría ni legitimaría la imposición de estas órdenes y medidas en contra de la Compañía [sic]. Lo anterior, habida cuenta de que, como la propia SIC reconoció ya en la Resolución No. 88509 de 5 de diciembre de 2018, mi representa no ostenta la calidad de Responsable del “Tratamiento de los datos [sic] recolectados por la aplicación ‘UBER’

Como el Despacho bien lo reconoce en la Resolución [sic] Impugnada [sic], lo que mi representada informó en su momento a la SIC fue que tenía acceso a una información limitada, y solamente para efectos de prestación de servicios de mercadeo, publicidad. De la misma manera, para la Dirección es claro que la Compañía sí actúa en algunas ocasiones como Encargado del Tratamiento por mandato expreso de Uber BV, circunstancia que de ninguna manera implica que le sean exigibles los deberes que en la presente actuación se asocian al Responsable del Tratamiento.

Además de lo anterior, en este punto, la investigada afirma que es la propia resolución impugnada la que evidencia que no hay razón, causa o derecho que justifique la imposición de estas órdenes y medidas en su contra:

lo anteriormente expuesto no fuera suficiente, resulta que es la propia Resolución Impugnada la que evidencia, por una parte, que nada de lo dicho en los numerales anteriormente mencionados es cierto. Y, por la otra, que, efectivamente, no hay razón, causa o derecho que justifique la imposición de estas órdenes y medidas en contra de la Compañía.

Una simple revisión de este acto administrativo da cuenta de ello, a saber:

- a. En el numeral 18.5.1 se hace referencia al sitio web [www.uber.com](http://www.uber.com), el cual no es propiedad de mi representada. De hecho, la Compañía no cuenta con ninguna página de internet, circunstancia que ya fue probada mediante un testigo experto ante los jueces y tribunales del país, cuya transcripción se aporta junto con este recurso.
- b. En el numeral 19.2.2 la propia Resolución Impugnada reconoce que Uber Technologies, Inc. es:
  - El propietario “de las Aplicaciones Móviles ‘UBER’”;
  - El responsable “de la política de privacidad y de las medidas de seguridad con respecto a la protección los (sic) datos personales que trata para sus propósitos comerciales”;
  - El que suscribió el contrato de computación en la nube con Amazon Web Services –“AWS” S3- donde se almacenan las copias de seguridad de las bases de datos de UBER.
- c. Adicional a lo anterior, en el numeral 19.2.3 la SIC vuelve a reconocer lo que ya había reconocido en la Resolución No. 88509 de 5 de diciembre de 2018: que Uber B.V. es quien tiene la calidad de Responsable del Tratamiento de los datos personales que se recolectan a través de la aplicación UBER.
- d. El considerando vigésimo hace referencia a unas supuestas “FALLAS DE SEGURIDAD DE UBER”, ninguna de las cuales tiene relación, directa o indirecta, con mi representada. Es decir, la Compañía ciertamente no incurrió ni tuvo injerencia ni responsabilidad en esas supuestas fallas a que hace referencia este considerando. Nótese cómo la Compañía informó -en el marco de otra investigación- que no conoció el incidente cuando ocurrió.

De hecho, en este considerando la SIC relata cómo, supuestamente, se presentó un acceso no autorizado a los datos personales almacenados en la nube AWS S3, cuyo contrato habría sido suscrito por Uber Technologies Inc. y no por mi representada, tal como se menciona en los numerales 19.2.2 y 20.1.4 de la Resolución Impugnada.
- e. Las actuaciones, órdenes y sanciones supuestamente proferidas por autoridades extranjeras, que se enlistan en el considerando vigésimo primero tampoco se refieren y/o relacionan, directa o indirectamente, con la Compañía, sino con otras sociedades.



Por la cual se resuelve un recurso de apelación

VERSIÓN PÚBLICA

Página 19 del recurso presentado

f. A lo largo del considerando vigésimo segundo la Resolución Impugnada da cuenta de como mi representada no ha hecho cosa distinta de colaborarle a la Dirección, entre otras, en el sentido de:



Ponerle de presente que otra sociedad es el Responsable del Tratamiento (numeral 22.2);

- Informarle cuál es la sociedad encargada de tratar los datos personales "que habrían estado involucrados en el incidente de seguridad de datos de 2016" (numeral 22.3); y

- Remitirle información que le suministró Uber B.V. (numeral 22.4).

g. Las medidas de seguridad a que hace referencia el último párrafo de la página 33 tampoco se relacionan con mi representada, ni fueron adoptadas por esta última, pues se trata de un asunto que no es de su responsabilidad y a lo cual no está obligada.

Página 20 del recurso presentado

La investigada, continúa la sustentación de su recurso aduciendo que no le corresponde responsabilidad alguna frente al Tratamiento de los Datos hecho en las aplicaciones UBER. Lo anterior debido a que no ostenta frente a dicha información la calidad del Responsable del Tratamiento, ni por sí misma ni conjuntamente con ninguna otra sociedad.

*"La indebida valoración de la condición de la compañía como si fuera un co-responsable [sic] frente al Tratamiento de la información recolectada en las aplicaciones UBER, lleva a la SIC a las conclusiones erradas que expone en el numeral 19.2.6 de la Resolución [sic] recurrida.*

*(...) la Compañía [sic] no dispone de medios, recursos y/o mecanismos a través de los cuales pueda dar cumplimiento a las órdenes impartidas mediante el artículo primero de la parte resolutive de la Resolución [sic] Impugnada [sic].*

**D. Violación de la confianza legítima de la Compañía**

En primer lugar, vale la pena recordar a la Superintendencia la colaboración que hasta el momento ha prestado mi representada en relación con el asunto objeto de investigación. En efecto, según se lee del propio texto de la Resolución Impugnada, la Compañía le informó a la SIC quién era el Responsable del Tratamiento, cuál es la sociedad encargada de tratar los datos personales "que habrían estado involucrados en el incidente de seguridad de datos de 2016" y, además, le remitió toda la información que le suministró Uber B.V.

De hecho, hasta donde le fue posible, y con el único ánimo de colaborarle a la Superintendencia, mi representada respondió todos los requerimientos de información efectuados por esta Autoridad.

Así pues, pese a que mi representada no se encontraba obligada, siempre ha buscado prestar la mayor colaboración posible con la SIC, inclusive suministrando información que no es de su propiedad ni se encuentra en su poder. Habría que ver cuántas sociedades colaboran con esta Autoridad, al punto de hacer todo cuanto está a su alcance por entregar información que no le pertenece, para dimensionar la importancia del grado de colaboración de mi representada para con la Superintendencia.

Página 22 del recurso presentado

*Por la cual se resuelve un recurso de apelación*

Por ende, tanto a través del intercambio de correspondencia, como de un acto administrativo, la propia SIC creó en la Compañía la confianza legítima de que no ostenta la calidad de Responsable del Tratamiento, se insiste, al punto de que el cargo único contenido en la Resolución No. 88509 le fue imputado a otra sociedad, precisamente, en su calidad de Responsable. Y de que, en consecuencia, mi representada no sería objeto de ningún procedimiento, orden o medida administrativa en relación con datos personales, excepción hecha de la orden de colaboración contenida en la Resolución No. 88509, la cual, en todo caso, deberá ser revocada una vez se resuelvan los recursos interpuestos en su contra.

No obstante lo anterior, ahora la SIC decide cambiar intempestivamente su posición, y, haciendo caso omiso de la existencia y efectos de la Resolución No. 88509, pretende vincular a la Compañía a una serie de órdenes y medidas que solamente pueden serle impartidas a quien ostente la calidad de Responsable del Tratamiento. Pero, en ningún caso, a quien, como mi representada, no lo es.

Página 23 del recurso presentado

La investigada insiste en que es manifiesta la violación de la confianza legítima en su caso, pues, pese a no tener la calidad de Responsable, tal como la propia SIC ya lo había reconocido, seis meses después, y de forma intempestiva, cambió de criterio al impartirle una serie de órdenes cuando incluso no tiene competencia para tal fin.

**E. Carencia actual de objeto del presente trámite administrativo por hecho superado**

*“(…) el presente trámite administrativo carece de objeto. Lo anterior, por razón de que en el presente asunto se configuró un hecho superado, conforme a los argumentos que a continuación se pasan a exponer.*

*(…) dicha figura es absolutamente aplicable a este procedimiento administrativo, por cuanto el supuesto objeto del mismo (...) desapareció, incluso, desde mucho antes del inicio de este trámite.*

*“En efecto, según se lee en el considerando vigésimo del acto en comento, la SIC hace referencia a lo que denomina el [sic] “el incidente de seguridad que afectó datos [sic] personales en custodia o posesión de UBER”, el cual, si bien no tienen relación alguna con mi representada, ni mucho menos compromete su responsabilidad, aparentemente ocurrió hacia finales del año 2016. Es más, como la propia Resolución [sic] Impugnada [sic] bien lo reconoce, después del 15 de noviembre de 2016 no ha habido accesos no autorizados a los datos que se recolectan a través de la aplicación UBER.*

*Por consiguiente, los hechos objeto de este trámite administrativo fueron debidamente superados desde noviembre de 2016, por el actuar voluntario de las respectivas empresas responsables.*

*(…) este trámite administrativo carece de objeto, por cuanto su finalidad se consiguió hace años ya, se insiste, sin necesidad de que ninguna autoridad, local o extranjera, intervenga a fin de impartirle órdenes y directrices a las sociedades responsables por los datos [sic] recolectados a través de la aplicación UBER.*

Por la cual se resuelve un recurso de apelación

(...) con posterioridad al 15 de noviembre de 2016, no volvió a ocurrir ningún incidente en relación con los datos [sic] personales recolectados a través de la aplicación UBER.

(...)”

**F. La SIC desvió sus propias atribuciones al expedir la Resolución [sic] Impugnada [sic]**

(...) contraviniendo las disposiciones que reflejan la necesidad [sic] mantener absoluta observancia del principio de legalidad, mediante la Resolución [sic] Impugnada [sic] se dictaron toda una serie de órdenes y medidas en contra de mi representada: (i) pese a que la Superintendencia carece de competencia para tal efecto; y (ii) sin haber agotado previamente un procedimiento administrativo.

En primer término, y como ya se explicó, la Dirección no es competente para impartirle órdenes a mi representada al amparo de lo dispuesto por el literal e) del artículo 21 de la Ley 1581 de 2012, como si la Compañía ostentara la calidad de Responsable. Lo anterior, se insiste, habida cuenta de que la Compañía no es Responsable del Tratamiento, circunstancia que, inclusive, también fue expresamente reconocida por la SIC mediante la Resolución No. 88509 de 2018.

No obstante esta irrefutable circunstancia, la SIC procedió a dictar las órdenes contenidas en la Resolución Impugnada en contra de mi representada. Y, como también se vio ya, lo hizo con base en unas consideraciones absolutamente falsas y contrarias a la realidad.

De otra parte, es un hecho irrefutable que la SIC expidió tales órdenes en contra de mi representada sin haber conducido un procedimiento administrativo que le permitiera adoptar tales determinaciones. ¿Cómo es posible que la Superintendencia llegue a las conclusiones que plasmó en la Resolución Impugnada sin haber tramitado el respectivo procedimiento administrativo? Y, sobre todo, ¿sin haber oído a las sociedades objeto de las órdenes y medidas, y sin haberles permitido ejercer su derecho de defensa?

El resultado de tal proceder es que la SIC actuó excediendo sus competencias y emitió unas órdenes y medidas sin haber corroborado la configuración de los méritos y requisitos para tal fin.

Página 28 del recurso presentado

Para la investigada hay un desconocimiento cierto, directo e injustificado de las competencias de la SIC como autoridad en materia de protección de Datos personales, en tanto no existe ninguna norma que le haya otorgado competencia a la superintendencia para dictar este tipo de órdenes y medidas contra quien, no ostenta la calidad de Responsable del Tratamiento.

**G. La Compañía [sic] no está en posibilidad de prestar su colaboración para cumplir las órdenes impartidas en el artículo tercero de la Resolución [sic]**

(...) resulta claro que no existe ningún fundamento jurídico que justifique que mi representada se haga acreedora de dicha Orden, habida cuenta de que no solamente no existe norma que la obligue, sino que, además, porque la SIC carece de competencia para impartirle dicha orden a la Compañía [sic].

Por la cual se resuelve un recurso de apelación

(...)

*En efecto, todo parece indicar que la Superintendencia [sic] no tuvo en cuenta que le está ordenando a mi representada que colabore respecto de actuaciones que dependen de otras personas jurídicas completamente diferentes a la Compañía [sic] (...)*

*(...) la SIC no pude [sic] pretender imponerle a mi representada una orden de prestar una colaboración que supone la ejecución de unos hechos que exceden de sobremanera su objeto social y su ámbito de control y capacidad, como si se tratara de una autoridad delegando sus funciones en otra (...)*"

### **Solicitud**

1. Revocar la resolución impugnada, dada su manifiesta ilegalidad.
2. Abstenerse de proferir órdenes en contra de la investigada, dentro del presente y/o cualquier otro asunto relacionado con Datos personales que se recolectan a través de la aplicación UBER.

**TERCERO.** Que, por medio de comunicación 19-40311-20<sup>2</sup> de 16 de agosto de 2019, **UBER COLOMBIA S.A.S.** presentó recurso de reposición y, en subsidio apelación en contra de la Resolución No. 21478 de 17 de junio de 2019, en el cual argumentó lo siguiente:

### **II. Fundamentos de Derecho**

*La Resolución No. 21478 de 17 de junio de 2019 debe ser revocada debido a que: (1) la Dirección de Investigación violó el debido proceso de Uber B.V. al haber expedido una Resolución sin seguir las reglas de procedimiento establecidas en la Ley 1437 de 2011 ("CPACA") ni darle la oportunidad a Uber B.V. de ejercer su derecho de defensa; (2) la SIC no tiene jurisdicción ni competencia sobre Uber B.V., por estar el Responsable del Tratamiento ubicado en el extranjero y no existir un tratado internacional que permita la aplicación extraterritorial de la Ley 1581 de 2012; y (3) actualmente no existen fundamentos de hecho para ordenar a Uber B.V. la adopción de medidas adicionales para reforzar la protección de los Datos personales de los usuarios de la aplicación Uber.*

#### **1. La Dirección violó el debido proceso Uber B.V.**

*"(...)*

*La Dirección de Investigación adoptó la decisión de fondo en el mismo acto administrativo en que inició la actuación contra Uber B.V. y ordenó notificarla por primera vez. Uber B.V., por consiguiente, no pudo presentar pruebas o argumentos con anterioridad a la adopción de la decisión de impartirle órdenes e instrucciones como consecuencia de un supuesto desconocimiento de la ley.*

*(...)*

<sup>2</sup> De conformidad con la certificación de 28 de agosto de 2019, expedida por la Secretaria General Ad.-Hoc (Coordinadora del Grupo de Notificaciones y Certificaciones) de la Superintendencia de Industria y Comercio, la Resolución No. 21478 de 17 de junio de 2019 fue notificada mediante aviso a UBER B.V., el 8 de agosto de 2019. Con lo cual, el término para presentar los recursos vencía el 23 de agosto de 2019. Así las cosas, los recursos se presentaron en la oportunidad procesal correspondiente.

*Por la cual se resuelve un recurso de apelación*

*En el presente caso, la Dirección de Investigación omitió las principales etapas del procedimiento que debía seguir, lo cual de plano vicia de nulidad e ilegalidad su actuación, y obliga a revocarla. La SIC únicamente siguió las etapas (i) y (v) listadas anteriormente, y pretermitió las demás.*

*La Dirección de Investigación no otorgó a Uber B.V. la posibilidad de pronunciarse sobre el inicio de la actuación, de presentar argumentos frente a la misma, de solicitar y aportar pruebas, de pronunciarse sobre las que se aducen en su contra, y de que su posición y defensa fuese tenida en cuenta en la decisión de fondo. Es decir, la dirección pretermitió todo el trámite que estaba obligada a seguir.*

*Lo anterior porque en el mismo acto en que inició la actuación y ordenó informar a Uber B.V. sobre un proceso en su contra, profirió decisión de fondo y condenó la conducta de Uber B.V., solo quedándole a ésta la posibilidad de interponer recurso de reposición y apelación contra una actuación en la que no participó. Tomar una decisión de fondo en la misma Resolución que inicia la actuación y en la que se ordena notificar por primera vez a un administrado es contrario a derecho e ignora el procedimiento del CPACA que debe seguir la Dirección de Investigación para proferir un acto administrativo, sancionatorio o no.*

*Esto, por sí solo, obliga a la SIC a revocar el acto administrativo recurrido.*

Página 5 del recurso presentado

*“(...)*

*Hacer un juicio de responsabilidad, establecer que una compañía tiene “fallas” en su política de seguridad -sin siquiera darle la oportunidad de defenderse-, y como consecuencia de ello imponerle cargas y órdenes, configura una actuación eminentemente sancionatoria que debe seguir el trámite establecido en el CPACA para estos trámites.*

*Pero incluso si no lo fuera y, en gracia de discusión, se aceptara que esta es un actuación administrativa no sancionatoria o “preventiva”, de igual forma la Dirección de Investigación tendría que seguir obligatoriamente el procedimiento administrativo común y principal del artículo 34 del CPACA, que exige el cumplimiento de todos los pasos descritos anteriormente [sic] para respetar el derecho de defensa (inicio de actuación, traslado, oportunidad para presentar pruebas y argumentos, y decisión de fondo).*

*(...)*

*En el presente caso se pretermitieron las etapas de toda actuación administrativa y el derecho de defensa. De hecho, las pruebas en que aparentemente la SIC basó su decisión (como son los comunicados de prensa de decisiones de autoridades extranjeras) ni siquiera obrarían en el expediente en castellano ni habrían sido traducidas al español por intérprete oficial (según los pues de página de la propia SIC en la Resolución), en contravía de las normas procesales, en especial del artículo 251 del CGP.*

*(...)*

**2. La Dirección de Investigación no tiene jurisdicción ni competencia sobre Uber B.V.**

*Por la cual se resuelve un recurso de apelación*

*“(...)*

*Uber B.V. es el Responsable del tratamiento [sic] de los datos [sic] personales de las cuentas de la aplicación Uber, tal y como se informa a los usuarios a través de la política de privacidad (...). No obstante, Uber B.V. no trata datos [sic] personales en el territorio colombiano y tampoco se encuentra ubicado en el territorio nacional.*

*Para que la ley le fuera aplicable a Uber B.V., sería necesaria la existencia de un tratado internacional que expresamente permitiera la aplicación de la Ley 1581 de 2012 a un Responsable domiciliado en Países bajos.*

*Dicho tratado internacional (...) no existe en el ordenamiento jurídico colombiano.  
(...)*

*En primer lugar, la SIC está declarando la existencia de un supuesto grupo empresarial sin tener competencia para ello, lo cual es facultad expresa de la Superintendencia de Sociedades, no de la SIC.*

*En segundo lugar, la SIC manifiesta que Uber B.V es parte del supuesto “grupo UBER” con fundamento en que en el certificado de existencia y representación legal de Uber Colombia S.A.S. se manifiesta que Uber Technologies Inc. Ejerce control indirecto sobre Uber Colombia S.A.S. a través de Uber Internacional C.V., Uber International B.V. y Uber International Holding B.V. No obstante, basta observar el certificado para darse cuenta de que Uber B.V. por ninguna parte aparece en el supuesto e hipotético grupo empresarial.*

*Uber International B.V. y Uber International Holding B.V. son sociedades diferentes a Uber B.V. que es el Responsable del tratamiento [sic]. La terminación “B.V.” simplemente hace referencia a un tipo societario en el país de domicilio, pero no implica que sea la misma sociedad registrada en el certificado de existencia y representación. ¿Cómo puede la SIC decir que Uber B.V. hace parte del mismo grupo empresarial con base en un certificado que ni siquiera la nombra?*

*En tercer lugar, incluso si Uber B.V. perteneciera a un supuesto grupo societario de Uber Colombia S.A.S. y Uber Technologies Inc. En los términos descritos por la SIC, ello tampoco tendría los efectos de aplicación normativa extraterritorial que pretende la SIC (...)*

El pertenecer a un grupo empresarial no elimina la limitación de responsabilidad societaria atribuida por la ley colombiana a una sociedad. El control societario en Colombia, desde el punto de vista legal, solo tiene los siguientes efectos:<sup>11</sup> (i) la obligación de inscribir el vínculo de control en el registro mercantil de la sociedad controlada; (ii) la consolidación de los estados financieros de las entidades vinculadas; (iii) la prohibición de imbricación (existencia de participaciones recíprocas de capital entre las matrices y sus subordinadas); y (iv) la presunción de responsabilidad de la sociedad controlante por la insolvencia de la sociedad controlada. Ninguna de ellas extiende la responsabilidad de la matriz al cumplimiento o no de una norma por parte de su subordinada, lo que implicaría el levantamiento del velo corporativo por una orden de la SIC.

No puede entonces la SIC usar un argumento de un supuesto Grupo empresarial para manifestar que a Uber B.V. le son aplicables las normas de protección de datos colombianas, ya que no solo no se nombra a Uber B.V. en el certificado de existencia y representación legal de Uber Colombia S.A.S., sino que incluso si existiera el grupo empresarial, ello no sería argumento para descender el velo corporativo en la aplicación de normas jurídicas colombianas a una empresa extranjera.

*Por la cual se resuelve un recurso de apelación*

Página 10 del recurso presentado

La investigada argumenta que aceptar la tesis de la Dirección de Investigación implica decir que la SIC tiene competencia para levantar el velo corporativo de una sociedad en Colombia, e incluso por causales que ni siquiera están contempladas en la Ley.

En conclusión, considera que la resolución recurrida debe ser revocada porque la SIC no tiene competencia respecto del Tratamiento de Datos personales que realiza Uber B.V., comoquiera que no existe ninguna norma o tratado internacional que permita la aplicación extraterritorial de la Ley 1581 de 2012 a Uber B.V., domiciliada en el extranjero.

**3. *No existen actualmente fundamentos de hecho que soporten la decisión adoptada por la SIC en el acto administrativo recurrido***

*Después del incidente sufrido a finales de 2016, Uber Technologies Inc. (UTI), en su condición de encargado del Tratamiento por cuenta de Uber B.V., adoptó las medidas necesarias y razonable para reforzar la seguridad y protección de los Datos personales que trata.*

*No se entiende por qué entonces la SIC profiere, casi dos años después de que UTI anunciara el incidente y casi tres años después de que se tomaran medidas correctivas frente al mismo), órdenes en contra de Uber B.V., cuando se han adoptado de tiempo atrás las medidas de seguridad para mitigar los riesgos potenciales sobre los datos [sic] personales relacionados con el incidente de seguridad, y que son objeto de tratamiento [sic] por la compañía.*

Por la cual se resuelve un recurso de apelación

VERSIÓN PÚBLICA

<b>Medidas tomadas por UTI con respecto al incidente de 2016</b>
<i>Medidas Técnicas adoptadas por UTI relacionadas con el incidente y con posterioridad a su ocurrencia</i>
<ul style="list-style-type: none"><li>• En relación con las <u>Credenciales de Acceso</u>:<ul style="list-style-type: none"><li>○ Después del incidente, UTI inmediatamente rotó la única clave no rotada que se encontró en Github (que fue la credencial utilizada por actores externos, y que les otorgó acceso a AWS S3)</li></ul></li> <li>• En relación con <u>GitHub</u>:<ul style="list-style-type: none"><li>○ UTI requirió una autenticación de doble factor para el acceso a todos los repositorios privados de Github de UTI;</li><li>○ UTI Migró el código remanente a un código de almacenamiento interno y eliminó Github, salvo para cuestiones como "código abierto" (open source).</li></ul></li></ul>

Página 11 del recurso presentado



Por la cual se resuelve un recurso de apelación

VERSIÓN PÚBLICA

- En relación con AWS:
  - UTI ya requirió una autenticación multifactor para las cuentas individuales de AWS;
  - Desde el incidente, UTI también implementó un sistema de autenticación multifactor para prácticamente todas sus cuentas de servicio AWS;
  - Existe en la actualidad un proyecto para desarrollar procesos y procedimientos adicionales para reforzar aún más la seguridad para datos guardados en AWS;
- Finalmente, se tomaron medidas para implementar una autenticación multifactor en las aplicaciones críticas de cara externa.

#### *Medidas Organizacionales de UTI*

- UTI terminó el contrato de trabajo de dos de los empleados que dieron respuesta al incidente de seguridad;
- UTI contrató a Matt Olsen, antiguo Director de la Agencia contra el Terrorismo de los Estados Unidos y experto en ciberseguridad, como Jefe de Seguridad de Uber;
- Nuevo Liderazgo: UTI no solo contrató a Matt Olsen como su "Chief Trust and Security Officer", sino que también contrató al veterano experto en privacidad Ruby Zefo, como su ChiefPrivacyOfficer, y a Simon Hania como su Data ProtectionOfficer.
- UTI reestructuró su equipo de respuesta a incidentes;
- Las medidas de seguridad para el uso de AWS fueron reforzadas, y los requerimientos de seguridad escritos de AWS fueron publicados;
- Los requisitos para el programa de "BoutBounty" de UTI fueron actualizados.

#### *Medidas Implementadas como respuesta directa al incidente*

- UTI revisó su código de repositorio de fuente interna para identificar y remover cualquier clave funcional remanente de acceso codificadas de AWS;
- UTI implementó un monitoreo de fraude para las cuentas impactadas;
- UTI actualizó su entrenamiento de claves seguras para los ingenieros con el objeto de tomar el incidente de 2016 como un ejemplo de por qué es importante no copiar secretos, incluyendo claves de AWS, en el código fuente de Uber;

#### *Otras medidas relacionadas de forma indirecta con el incidente*

- Se realizaron entrenamientos adicionales para el equipo de respuesta de seguridad. Así, por ejemplo, entre el 1 de marzo y el 24 de mayo de 2019, se realizaron clases obligatorias para

Por la cual se resuelve un recurso de apelación

VERSIÓN PÚBLICA

los miembros del equipo de intrusión de SRL.

*Mejoras en seguridad de datos no relacionadas con el incidente*

- Además de las medidas adoptadas para el incidente de 2016, en 2018 Uber B.V. y UTI actualizaron sus planes de respuesta a incidentes para asegurar que las medidas apropiadas sean tomadas en el evento de un incidente.
- UTI ha desarrollado nuevos procesos y equipos para reforzar su capacidad de detectar y responder a amenazas de ciberseguridad.
  - El Equipo de Respuestas a Amenazas terceriza la selección previa de cualquier potencial amenaza de incidente de seguridad a un centro de operaciones de seguridad que trabaja 24/7. Esto ha resultado en una reducción significativa del tiempo que toma involucrarse y mitigar cualquier actual o potencial riesgo de incidente de seguridad.
  - El equipo de amenazas de seguridad también ha creado un equipo con dedicación especializada denominado Equipo de Detección de Amenazas, que ha desarrollado y mantendrá reglas de detección para identificar de forma proactiva cualquier actividad sospechosa o maliciosa en el negocio de Uber.
  - De igual forma, UTI ha creado un Equipo Rojo dentro del Equipo de Detección de Amenazas que, actuando en el rol de un intruso simulado, realiza test de penetración (entre otros), para proactivamente identificar y remediar cualquier debilidad de seguridad y continuamente realizar mejoras en seguridad a lo largo del negocio de Uber.
  - Finalmente, UTI ha creado un equipo especializado de Inteligencia en Amenazas, que tiene la tarea de desarrollar y mantener un profundo entendimiento de las amenazas actuales o potenciales que puede tener Uber en su actual ambiente de operación y entregar inteligencia proactiva frente a amenazas a sus grupos de interés para asegurar medidas de seguridad apropiadas e implementar estrategias de mitigación del riesgo.
- A principios de este año, los productos de Uber B.V., incluyendo Uber para Negocios fueron certificados conformes con ISO/IEC 27001. Esta certificación refleja los pasos significativos que ha dado Uber B.V. y continúa dando para implementar controles de administración de seguridad en su negocio.
- Uber ha ajustado sus políticas escritas frente a seguridad en la información. Estas nuevas políticas están alineadas con ISO/IEC 27001/27002.
- Mejoras al Proceso de Desarrollo de Software Seguro
  - Se ha reforzado la seguridad y privacidad en el diseño, con la incorporación de Evaluaciones de Impacto y Revisiones de Seguridad en la fase de diseño del desarrollo del ciclo de software para identificar mejor los riesgos de seguridad y privacidad así como proveer mayores guías de seguridad y privacidad a los

Por la cual se resuelve un recurso de apelación

VERSIÓN PÚBLICA

ingenieros:

- Entrenamiento adicional
  - Recientemente Uber desplegó un entrenamiento en privacidad y seguridad con el Instituto SANS para ciertos trabajadores, que incluyó módulos sobre ataques, ingeniería social, phishing, y software malicioso.

Página 14 del recurso presentado

La recurrente afirma que, las medidas adoptadas fueron idóneas y proporcionales para los sistemas de información de Uber, y redujeron el potencial de incidentes futuros que afectarían el derecho de *habeas data* para los Titulares de cuentas de Uber en Colombia.

Así pues, informa que, los controles implementados, combinados con la investigación realizada por Uber en 2016 (que incluyó) la identificación de los actores externos y confirmación de que borrarían los Datos que obtuvieron) resultaron efectivos, al punto que:

- (i) Las cuentas de Uber involucradas en el incidente ocurrido en 2016, han sido monitoreadas, y no hay evidencia alguna de inicios de sesión no autorizados, fraude o mal uso por parte de un tercero;
- (ii) No se ha recibido ninguna queja formal de algún usuario de la plataforma de Uber en Colombia o algún proceso judicial que tenga relación con el incidente; y
- (iii) No hay evidencia sobre alguna violación al derecho de *habeas data* de los Titulares de información personal en Colombia.

Los controles de seguridad establecidos están diseñados para proteger los datos que trata Uber B.V. De hecho, esos controles han sido presentados a la autoridad que tiene jurisdicción sobre Uber B.V.

No existe entonces en la actualidad un fundamento de hecho para la Resolución de la SIC. La desaparición de los presupuestos de hecho en los que se fundamenta un acto administrativo es una causal de pérdida de ejecutoria del mismo. En este evento, el acto administrativo nació sin fundamento de hecho, en la medida en que Uber B.V. de tiempo atrás adoptó las medidas necesarias y razonables para proteger adecuadamente los datos de sus usuarios, siguiendo estándares internacionales, y presentó a la SIC dichas medidas en actuaciones administrativas diferentes ante la Dirección de Investigación.

La Resolución, por consiguiente, ignora que Uber B.V. ya adoptó de tiempo atrás las medidas necesarias y razonables para mitigar potenciales riesgos futuros. El haber omitido tal situación y adoptar medidas que resultan a todas luces desproporcionadas frente a lo ya hecho por Uber B.V., a través de su encargado UTI, en sus procedimientos y prácticas de seguridad de la información, es resultado de no haber otorgado a la compañía la facultad de pronunciarse y presentar pruebas en la actuación administrativa antes de adoptarse la decisión de fondo.

Página 14 del recurso presentado

## Solicitud

1. Revocar la resolución impugnada, en virtud de que:
  - La Dirección de Investigación violó el debido proceso de Uber B.V. al haber expedido una resolución sin seguir las reglas de procedimiento establecidas en la Ley 1437 de

*Por la cual se resuelve un recurso de apelación*

2011 (“CPACA”), ni darle la oportunidad a Uber B.V. de ejercer su derecho de defensa;

- La SIC no tiene jurisdicción ni competencia sobre Uber B.V., por estar el Responsable del Tratamiento ubicado en el extranjero y no existir un tratado internacional que permita la aplicación extraterritorial de la Ley 1581 de 2012; y
- Actualmente no existen fundamentos de hecho para ordenar a Uber B.V. la adopción de medidas adicionales para reforzar la protección de los Datos personales de los usuarios de la aplicación Uber.

2. Archivar la actuación administrativa No. 19-40311.

**CUARTO.** Que por medio de la Resolución No. 47593 de 18 de agosto de 2020, 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. 21478 de 17 de junio de 2019, se procede a resolver el recurso apelación interpuesto, de acuerdo con las siguientes,

#### **CONSIDERACIONES DEL DESPACHO**

##### **1. 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 la cual se resuelve un recurso de apelación*

Por su parte, el artículo 16 del Decreto 4886 de 26 de diciembre de 2011<sup>3</sup> establece las funciones del Superintendente Delegado para la Protección de Datos Personales, entre las cuales se destacan las siguientes:

“(…)

*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.*

(…)”

## **2. DEL EXAMEN PROCESAL REALIZADO POR LA DIRECCIÓN DE INVESTIGACIÓN DE DATOS PERSONALES A LOS RECURSOS INTERPUESTOS**

En la Resolución No. 47593 de 2020 la Dirección de Investigación de Datos Personales precisó:

**SÉPTIMO:** Que, dentro del término legal previsto para el efecto y una vez analizados los requisitos del artículo 77 de la Ley 1437 de 2011, con base en lo expuesto por el recurrente, este Despacho hará las siguientes consideraciones:

Frente a los argumentos presentados por la sociedad recurrente (UBER COLOMBIA SAS) se encuentra que los mismos se concretan en los siguientes aspectos, a saber: (i) la naturaleza del Responsable y del Encargado del Tratamiento; (ii) la alegada falta de competencia para ejercer funciones de vigilancia y control; (iii) la supuesta violación del debido proceso de la sociedad UBER COLOMBIA SAS; (iv) la falsa motivación de la Resolución recurrida; (v) sobre la naturaleza de las órdenes; (vi) sobre la aplicación de la teoría del hecho superado (vii) sobre la aplicación de los principios contenidos en CPACA en las actuaciones administrativas de esta entidad; (viii) sobre el deber de colaboración y (ix) la pretensión.

Por su parte, los argumentos esgrimidos por la segunda sociedad recurrente (UBER B.V.) se enmarcan en los aspectos, a saber: (i) la indebida notificación de la resolución objeto de análisis; (ii) la falta de competencia de esta entidad para proferir las órdenes del caso, (iii) la alegada falta de fundamentos de hecho que motivo la expedición de las órdenes y (iv) la pretensión. Finalmente, se analizará un supuesto incidente de nulidad en la actuación administrativa interpuesto por esta última sociedad.

Hoja 11 del Acto Administrativo No. 47593 de 2020

De esta manera, y luego de realizar el análisis pertinente sobre los **argumentos** presentados por los recurrentes, y los documentos que reposan en el expediente esta Delegatura se sujeta a lo allí decidido en lo relacionado con:

### **A. Uber Colombia S.A.S.:**

- (i) Falta de competencia para ejercer funciones de vigilancia y control;
- (ii) Violación del debido proceso de la sociedad Uber Colombia S.A.S.;
- (iii) Falsa motivación de la resolución recurrida;
- (iv) Hecho superado;
- (v) Aplicación de los principios contenidos en el CPACA en las actuaciones administrativas de la Superintendencia de Industria y Comercio;

<sup>3</sup> 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.

*Por la cual se resuelve un recurso de apelación*

**B. Uber B.V.**

- (i) Indebida notificación de la resolución recurrida;
- (ii) De la nulidad; y,
- (iii) Falta de competencia de esta autoridad para proferir las órdenes del caso

Vale la pena reiterar lo referente a la aplicación de la Ley colombiana a UBER B.V.

- **La Ley 1581 de 2012 es aplicable a UBER B.V. 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 solo se menciona en el artículo 15 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:

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 :

*“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” .*

Mediante la Resolución 47593 de 2020 se puso de presente lo siguiente:

Por la cual se resuelve un recurso de apelación

El tratamiento de datos por parte de la plataforma sucede también mediante la instalación de *cookies* (ficheros automáticos de información) en los dispositivos de los usuarios de la plataforma. Las *cookies* son pequeños paquetes de información enviados desde sitios web y almacenados en los computadores, los cuales permiten identificar la actividad de navegación en internet por parte de una persona, incluidos los clics, la información que la persona diligencia en formularios, los inicios de sesión de aplicaciones o cuentas, etc.

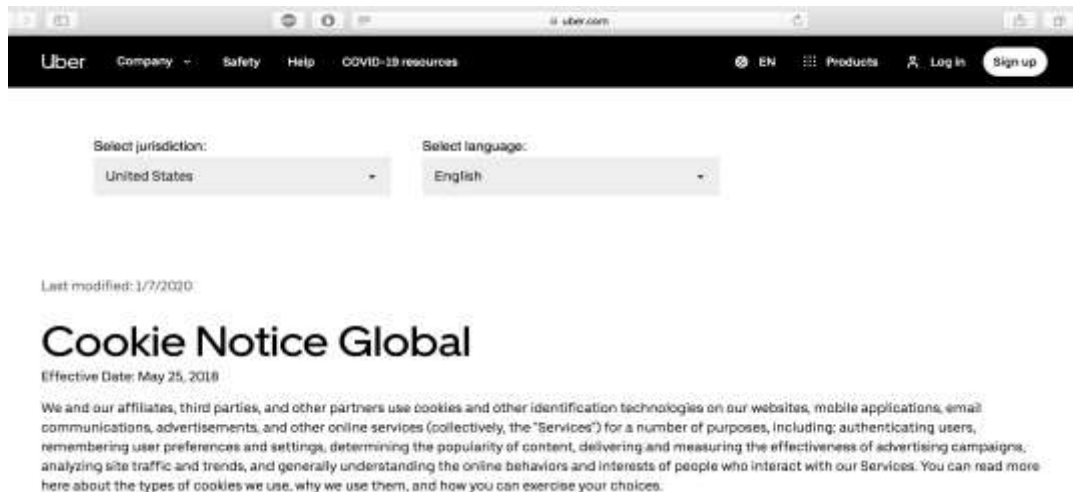
Cuando un usuario inicia sesión en "[www.uber.com](http://www.uber.com)", o hace cualquier tipo de uso o interacción con los servicios de UBER, se almacenan *cookies* en su computador o en cualquier dispositivo móvil que use: Tableta, celular inteligente, etc.

El uso de *cookies* por la Plataforma está explicado en su "política de *cookies*":

*"(...) Nosotros y nuestros afiliados, terceros y otros socios utilizamos cookies y otras tecnologías de identificación en nuestros sitios web, aplicaciones móviles, comunicaciones electrónicas, anuncios y otros servicios en línea (conjuntamente, los "Servicios") para una serie de propósitos, entre los que se incluyen: autenticación de usuarios, recordar las preferencias y la configuración del usuario, determinar la popularidad de los contenidos, entrega y medición de la efectividad de las campañas publicitarias, analizar el tráfico del sitio y las tendencias y, en general, para la comprensión de los comportamientos e intereses en línea de las personas que interactúan con nuestros Servicios (...) Las cookies suministradas por empresas que no operan el dominio que usted está visitando se llaman "cookies de terceros". Así, podemos permitir a Google poner una cookie en su navegador mientras visita [www.uber.com](http://www.uber.com), y esa sería una cookie de terceros. Las cookies también pueden perdurar durante diferentes períodos de tiempo. Las "cookies de sesión" solo duran mientras su navegador esté abierto. Estas se eliminan automáticamente una vez que cierra su navegador. Otras cookies son "cookies persistentes", lo que significa que sobreviven después de que su navegador se cierra. Por ejemplo, pueden reconocer su dispositivo cuando vuelve a abrir el navegador y navega de nuevo por Internet. (...) Usted tiene el derecho de elegir si desea o no aceptar las cookies. Sin embargo, son una parte importante de cómo funcionan nuestros Servicios, por lo que debe ser consciente de que si decide rechazar o eliminar las cookies, esto podría afectar la disponibilidad y funcionalidad de los Servicios."*<sup>423</sup>

(énfasis añadido).

Lo anterior fue verificado consultando la "Cookie Notice Global"<sup>4</sup> de UBER que dice lo siguiente:



UBER B.V. usa "cookies" para recolectar o tratar datos personales en el Territorio de la República de Colombia. Autoridades de protección de Datos de otros países 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.

<sup>4</sup> Cfr. <https://www.uber.com/legal/en/document/?name=cookie-notice&country=united-states&lang=en> . Última consulta: septiembre 28 de 2020

*Por la cual se resuelve un recurso de apelación*

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” . (...). (Destacamos).*

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 Personales. Por lo tanto, UBER B.V. recolecta y trata datos personales en el territorio colombiano, razón por la cual debe cumplir la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias.

**3. 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 que *“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 personales, tales como la recolección, almacenamiento, uso, circulación o supresión.”***<sup>5</sup>

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 lo 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

<sup>5</sup> Cfr. Literal g) del artículo 4.



*Por la cual se resuelve un recurso de apelación*

medios manuales<sup>6</sup> 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 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, conocido o por conocer, y para cualquier tema. El tratamiento puede efectuarse mediante cualquier medio, sin que refiera o limite a tecnologías, procesos o medios tecnológicos específicos.

#### **4. DE LA FACULTAD LEGAL PARA IMPONER LAS ÓRDENES CONTENIDAS EN LA RESOLUCIÓN No. 21478 DE 17 DE JUNIO DE 2019**

En el recurso interpuesto se argumentó que esta entidad no tiene las facultades legales para imponerle a la investigada las órdenes impartidas mediante la Resolución No. 21478 de 17 de junio 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*

<sup>6</sup> 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.

*Por la cual se resuelve un recurso de apelación*

*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 los recurrentes 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.

##### **5. DEL CONTEXTO DE LAS ÓRDENES IMPARTIDAS EN RELACIÓN CON LA OCURRENCIA DEL INCIDENTE DE SEGURIDAD**

Es importante recordar que, tal como lo precisó la recurrente, Uber Colombia S.A.S., sí trata Datos personales de usuarios colombianos:

*“(…) la Compañía [sic] tiene acceso a información limitada sobre usuarios-pasajeros y usuarios-conductores registrados en la aplicación y/o plataforma tecnológica “UBER”, aprovechable desde Colombia. El rol de mi representada con relación a algunos datos [sic] que se tratan a través de la aplicación y/o plataforma tecnológica*

*Por la cual se resuelve un recurso de apelación*

*“UBER”, en Colombia, es el de Encargado del Tratamiento, obrando frente a los mandatos recibidos por parte de Uber BV. (...)*

Asimismo, nos referimos al comunicado presentado por Dara Khosrowshahi (*Chief Executive Officer* de Uber), en el cual informó, además de la ocurrencia del incidente de seguridad, lo siguiente:

*“(...) a finales de 2016 dos individuos ajenos a la Compañía obtuvieron de forma inapropiada acceso a datos de usuarios almacenados en un servidor en la nube alojado por un proveedor externo que utilizábamos.*

*(...) los individuos pudieron acceder a archivos que contenían una cantidad significativa de otra información, entre la que se incluye:*

- Los nombres y los números de licencia de conducir de cerca de 600,000 socios conductores en Estados Unidos. Ellos pueden encontrar más información [aquí](#).*
- Información personal de 57 millones de usuarios alrededor del mundo, incluyendo a los socios conductores mencionados anteriormente. Esta información incluye nombres, direcciones de correo electrónico y números de teléfono. Los usuarios pueden encontrar más información [aquí](#).*

*Al momento del incidente, tomamos medidas de inmediato para asegurar los datos y bloquear cualquier acceso no autorizado. Al mismo tiempo, identificamos a los atacantes y nos aseguramos que los datos descargados fueran destruidos. Además, implementamos medidas de seguridad para restringir accesos y fortalecer los controles en nuestras cuentas de almacenamiento de datos en la nube.*

***Puede que muchos se pregunten por qué estamos hablando de esto ahora, un año después de ocurrido el incidente.*** Yo me hice la misma pregunta, así que inmediatamente solicité una investigación acuciosa acerca de lo ocurrido y cómo lo manejamos. Lo que descubrí, particularmente acerca de nuestra falla a la hora de notificar a las personas y a las autoridades el año pasado, me ha llevado a adoptar varias medidas:

- He solicitado a [Matt Olsen](#), co-fundador de una firma consultora de ciberseguridad, ex consejero general de la Agencia Nacional de Seguridad de EE.UU. y director del Centro Nacional para el Contraterrorismo, que me ayude a analizar cómo podemos guiar y estructurar nuestros equipos de seguridad y decidir nuestros siguientes pasos. Con efecto inmediato, dos de las personas que lideraron la respuesta a este incidente, no seguirán relacionados a la Compañía.*
- Estamos notificando individualmente a los socios conductores cuyos números de licencia de conducir fueron descargados.*
- Estamos ofreciendo a estos conductores servicio gratuito de servicios de verificación de crédito y protección ante robo de identidad.*
- Estamos notificando a las autoridades regulatorias.*
- Si bien no hemos visto evidencia de fraude o uso indebido relacionado a este incidente, estamos monitoreando las cuentas afectadas y las hemos notificado para brindarles protección adicional ante fraudes.*

*Nada de esto debió haber ocurrido, y no intentaré justificarlo. Si bien no puedo borrar el pasado, sí puedo comprometerme a nombre de cada empleado de Uber a que aprenderemos de estos errores. **Estamos cambiando la forma en que trabajamos,***

*Por la cual se resuelve un recurso de apelación*

**poniendo la integridad en el centro de cada decisión y esforzándonos para ganar la confianza de nuestros clientes**<sup>7</sup>. (Destacamos y resaltamos).

Lo que se quiere relieves y privilegiar es que, si hubo un reconocimiento expreso por parte de Uber del incidente de seguridad (un año después de ocurrido), situación que es notoriamente conocida y de la cual, según Dara Khosrowshahi (Chief Executive Officer de Uber) existe un compromiso por parte de esa compañía para evitar un nuevo suceso de este tipo. No entiende este despacho, cuál es la resistencia generalizada por parte de las recurrentes a cumplir la orden impartida, la cual, en todo caso es de carácter **preventivo** para evitar que se afecte la seguridad de los Datos de los colombianos.

La seguridad es un tema que no solo afecta a los Titulares de los Datos, sino a los intereses de las empresas porque de ello depende la protección de sus activos, su reputación, su buen nombre y la confianza que genera en el mercado, el ciberespacio y en los diferentes países en donde opera cualquier organización seria y comprometida con la legalidad y el buen trato de la información de sus empleados y sus clientes.

## 6. 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 las recurrentes.

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.

## 7. LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO NO HA DESESTIMADO LA PERSONALIDAD JURÍDICA DE LA SOCIEDAD RECURRENTE

Al respecto, **es necesario precisar que esta superintendencia** se limitó a impartir unas órdenes a las sociedades **UBER TECHNOLOGIES, INC., UBER COLOMBIA SAS** [sic] y **UBER B.V.**, Sin embargo, se aclara que esta autoridad en ningún momento ha ordenado el levantamiento del velo corporativo de ninguna de esas compañías

<sup>7</sup> <https://www.uber.com/es-CO/newsroom/incidente-de-seguridad-de-datos-en-2016/>

*Por la cual se resuelve un recurso de apelación*

En este sentido, y en relación con las conductas que no ha adelantado esta autoridad, cobra especial relevancia resaltar que la misma:

- i. Carece de competencia para declarar la desestimación de la personalidad jurídica de cualquier sociedad. Lo anterior, de conformidad con lo dispuesto en el literal d) del numeral 5 del artículo 24 del Código General del Proceso<sup>8</sup>;
- ii. No ha declarado ninguna responsabilidad patrimonial como consecuencia de las órdenes impartidas por medio de la expedición de la Resolución No. 21478 de 17 de junio de 2019; y,
- iii. En el desarrollo de este proceso administrativo no se ha impuesto ninguna carga patrimonial ninguna de las empresas del Grupo Uber.

**8. UBER COLOMBIA S.A.S. EN CONCURSO CON UBER B.V. 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**

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*”<sup>9</sup>.

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 incluye, además de la Carta Superior, el sometimiento a la ley en general, así como a las órdenes de autoridades administrativas, entre otras.

**PRINCIPIO DE PRIMACÍA DE LA REALIDAD SOBRE LAS FORMAS**

El artículo 53 de la Constitución Política Nacional es el fundamento jurídico de este principio. Según la Corte Constitucional, “*La primacía de la realidad sobre las formalidades establecidas por los sujetos de las relaciones laborales, es un principio constitucional (...) El mencionado principio agota su cometido al desentrañar y hacer triunfar la relación de trabajo sobre las apariencias que hayan querido ocultarla..*”<sup>10</sup>

<sup>8</sup> “(...)

5. *La Superintendencia de Sociedades tendrá facultades jurisdiccionales en materia societaria, referidas a:*

(...)

d. *La declaratoria de nulidad de los actos defraudatorios y la desestimación de la personalidad jurídica de las sociedades sometidas a su supervisión, cuando se utilice la sociedad en fraude a la ley o en perjuicio de terceros, los accionistas y los administradores que hubieren realizado, participado o facilitado los actos defraudatorios, responderán solidariamente por las obligaciones nacidas de tales actos y por los perjuicios causados. Así mismo, conocerá de la acción indemnizatoria a que haya lugar por los posibles perjuicios que se deriven de los actos defraudatorios”.*

<sup>9</sup> “*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

<sup>10</sup> Cfr. Corte Constitucional, sentencia C-555 de 1994. M.P. Dr. Eduardo Cifuentes Muñoz

*Por la cual se resuelve un recurso de apelación*

De conformidad con este principio, prima la realidad material sobre las formalidades o apariencias jurídicas. La aplicación del mismo implica desestimar la forma y las apariencias e imponer la materialidad de lo que sucede en la práctica.

Este principio no solo es aplicable a la relaciones laborales sino a otras situaciones. En este sentido, en relación con otros campos del derecho, la Corte Suprema de Justicia, en Sentencia de 24 de julio de 2012 (radicado No. 2005-00595-01), consideró que:

*“Para averiguar el querer de los obligados, a más del tenor literal de sus cláusulas y las directrices establecidas en los artículos 1618 a 1624 del Código Civil, 5 y 823 del Código de Comercio, debe tener en cuenta el intérprete diversos factores que inciden en el acuerdo, tales como las condiciones particulares de los intervinientes y su proceder en los diferentes momentos contractuales, esto es, antes, durante y después de su celebración, de tal manera que se refleje de manera precisa el ánimo que los inspiró a vincularse (...).”*

Dado lo anterior, para este Despacho es relevante determinar lo que ocurre en la realidad y lo que se ha definido “formalmente” entre las empresas en cuestión. Así pues, en este caso, se dio prevalencia a lo que ha pasado en la práctica entre Uber Colombia S.A.S. y las demás compañías que conforman el Uber.

Sin embargo, llama la atención del Despacho que la recurrente afirme con tal vehemencia que la misma no es “propietaria, arrendataria, licenciataria, beneficiaria, usuaria, administradora o responsable de la aplicación UBER”, puesto que dicha circunstancia es distinta a la realidad fáctica, en la medida en que la sociedad genera beneficios y rendimientos de carácter económico para su funcionamiento a partir del servicio que presta de conectar al conductor con el eventual usuario de la plataforma tecnológica.

En esta medida, es claro que la sociedad UBER COLOMBIA S.A.S debe acatar la normatividad nacional sobre protección de datos personales y que no puede excusarse en que la misma no goza de estas características “propietaria, arrendataria, licenciataria, beneficiaria, usuaria, administradora o responsable de la aplicación UBER”, puesto que tal argumento implicaría que la sociedad actúa simplemente como una sociedad meramente operativa, situación contraria a la realidad y que permite afirmar que dicha sociedad no respeta el derecho fundamental a la protección de datos personales.

Hoja 14 del Acto Administrativo No. 47593 de 2020

Es bien conocido el aforismo del derecho que señala, “*las cosas son lo que su naturaleza y no lo que su denominación determina*”. O, lo que es igual, el principio de irrelevancia del *nomen iuris*, o principio de primacía de la realidad (las cosas son lo que son y no lo que las partes dicen que son).

Ahora bien, no se desconoce la libertad que tienen las empresas de diseñar su estrategia corporativa o societaria, pero ello no es óbice para desconocer sus responsabilidades frente a la protección y garantía de derechos constitucionales fundamentales como la protección de datos personales.

## **9. DE LA RELACIÓN JURÍDICA DE UBER COLOMBIA S.A.S. CON UBER B.V. RESPONSABILIDAD DEL TRATAMIENTO DE DATOS PERSONALES DE LOS USUARIOS DE LA PLATAFORMA EN COLOMBIA**

*Por la cual se resuelve un recurso de apelación*

Como quedó demostrado en sede de reposición, y lo comprobó este despacho al analizar los documentos que hacen parte del expediente, Uber Colombia S.A.S. de acuerdo con la actividad económica y comercial que realiza: trata Datos de los Titulares de la información al obtenerlos con el fin de lograr conectar un socio conductor con un usuario del servicio.

En relación con este argumento de la recurrente, *“La indebida valoración de la condición de la compañía como si fuera un co-responsable [sic] frente al Tratamiento de la información recolectada en las aplicaciones UBER, lleva a la SIC a las conclusiones erradas que expone en el numeral 19.2.6 de la Resolución [sic] recurrida”*. La Sentencia C-748 de 2011 se refirió al tema de la responsabilidad solidaria en los siguientes términos:

*“(…) tanto el responsable como el encargado del tratamiento tienen responsabilidades claras, concretas y precisas frente al titular del dato, por cuanto ambos sujetos, en los términos de los preceptos en análisis, están obligados a garantizar el ejercicio pleno y efectivo del derecho al habeas data, el cual se irradia por todos los principios que rigen el tratamiento de datos (...)*

*(…) tanto el responsable como el encargado del tratamiento tienen una responsabilidad concurrente frente a la veracidad, integridad, finalidad e incorporación del dato, si se tiene en cuenta que la recolección y procesamiento de datos no es una actividad neutra que impida al encargado del tratamiento responder, incluso por la veracidad de la información sujeta a proceso, pues a éste le corresponde cerciorarse que se cumplan los requisitos para que un dato personal pueda ser objeto de tratamiento.*

***En consecuencia, la Sala advierte que si no se puede identificar de forma clara la posición de uno y otro, tendrán que responder de forma solidaria y no podrán excusar sus deberes de actualización, rectificación y exclusión o supresión del dato.***

*(…) lo importante para una verdadera garantía del derecho al habeas data, es que se pueda establecer de manera clara la responsabilidad de cada sujeto o agente en el evento en que el titular del dato decida ejercer sus derechos. Cuando dicha determinación no exista o resulte difícil llegar a ella, las autoridades correspondientes **habrán de presumir la responsabilidad solidaria de todos**, aspecto éste sobre el que guarda silencio el proyecto de ley y que la Corte debe afirmar como una forma de hacer efectiva la protección a la que se refiere el artículo 15 de la Carta”.*

Así las cosas, no le es dable a la recurrente obviar sus obligaciones en materia de protección de Datos personales.

### **¿Cómo participa Uber Colombia S.A.S. en el Tratamiento de Datos personales a través de la aplicación UBER en territorio colombiano?**

Es imposible ignorar el grado de subordinación que existe en las compañías del Grupo Uber. De hecho en el certificado de cámara de comercio de Uber Colombia S.A.S. se registró lo siguiente:

Por la cual se resuelve un recurso de apelación

SITUACIÓN DE CONTROL Y/O GRUPO EMPRESARIAL

Que por Documento Privado No. sin num de Representante Legal del 5 de agosto de 2016, inscrito el 11 de agosto de 2016 bajo el número 02131258 del libro IX, comunicó la sociedad matriz:

- UBER TECHNOLOGIES, INC.

Domicilio: (Fuera Del País)

Presupuesto: Numeral 1 Artículo 261 del Código de Comercio

Que se ha configurado una situación de control con la sociedad de la referencia.

Fecha de configuración de la situación de control : 2013-10-15

Se Aclara la Situación de Control, de fecha 5 de agosto de 2016, inscrita el 11 de agosto de 2016, bajo el No. 02131258 del libro IX, en el sentido de indicar que la sociedad UBER TECHNOLOGIES INC (matriz), comunica que ejerce situación de control indirecta sobre UBER COLOMBIA SAS (SUBORDINADA) A TRAVES DE LAS SOCIEDADES UBER INTERNATIONAL C.V, UBER INTERNATIONAL B.V Y UBER INTERNATIONAL HOLDING B.V.

Con esto, se evidencia el poder que ejerce el Responsable del Tratamiento de Datos personales en Estados Unidos de Norteamérica, Uber Technologies Inc. sobre Uber Colombia S.A.S (sociedad subordinada). En virtud de lo anterior, es posible concluir la existencia de una coordinación y control de la operación empresarial mediante la recepción de instrucciones y órdenes en las actividades que las compañías en cuestión desarrollan, y las cuales vienen del mismo administrador societario, Uber Management B.V.

Sobre este interrogante se pronunció la Dirección de Investigación de Protección de Datos Personales en el Acto Administrativo No. 47593 de 2020.

De esta manera, al acreditar que existe control interno por participación<sup>11</sup>, se puede concluir que este no es meramente formal. Según el artículo 260 de nuestro Código de Comercio, la subordinación implica que el **poder de decisión** de la compañía subordinada se encuentre sometido a la voluntad de la compañía matriz o controlante:

*“Subordinación. Una sociedad será **subordinada o controlada** cuando su **poder de decisión** se encuentre **sometido a la voluntad de otra u otras personas que serán su matriz o controlante**, bien sea directamente, caso en el cual aquélla se denominará filial o con el concurso o por intermedio de las subordinadas de la matriz, en cuyo caso se llamará subsidiaria.”. (Énfasis añadido).*

No puede desconocerse que, cuando la ley se refiere al poder de decisión, y a la voluntad de la controlante, se fija una relación de poder y determinación en la que la subordinada, realiza sus acciones principales con la aquiescencia de su controlante.

**Lo anterior es aun más certero, cuando la relación no se deriva de cualquier participación accionaria superior al cincuenta por ciento (50%), sino al ciento por ciento (100%) de las acciones de la subordinada.**

<sup>11</sup> Control interno por participación: Se verifica cuando se posea más del cincuenta por ciento (50%) del capital en la subordinada, sea directamente o por intermedio o con el concurso de las subordinadas, o las subordinadas de estas. Recuperado de [https://www.supersociedades.gov.co/delegatura\\_ivc/CartillasyGuias/Guia\\_Practica\\_RegimenMatricesySubordinadas.pdf](https://www.supersociedades.gov.co/delegatura_ivc/CartillasyGuias/Guia_Practica_RegimenMatricesySubordinadas.pdf) el 19 de enero de 2019.



*Por la cual se resuelve un recurso de apelación*

Es inocultable que Uber Colombia S.A.S., en el territorio de la República de Colombia, es una extensión de Uber B.V.; Uber Technologies Inc.; Uber Management B.V y Uber International Holding B.V. Lo anterior, sin perjuicio de la verificación de los requisitos establecidos en el artículo 469 y siguientes del Código de Comercio.

**Del análisis de la relación entre las anteriores compañías, esta autoridad colige, sin lugar a dudas, que sí existe una relación material en la que el poder de decisión de Uber Colombia S.A.S. depende de la voluntad de su controlante, Uber Technologies Inc. y, a su vez, de la controlante de esta, Uber B.V.**

Resulta por ello indiscutible que, Uber Colombia S.A.S. es una extensión real de la voluntad y finalidad económica de las compañías mencionadas en el territorio de la República de Colombia. Ocultarlo, además de insensato, desconocería que tienen un único propósito, el cual es servir económica y misionalmente a todo el grupo.

Como corolario de este razonamiento, la Superintendencia de Sociedades por medio del Concepto 220-002605 de 15 de enero de 2018 dispuso que:

*“(...) Entre dos sociedades, una extranjera y su filial colombiana, puede darse la situación de control, en tanto que aquella ejerza el poder de decisión sobre la colombiana; y, adicionalmente, puede configurarse la situación de Grupo Empresarial, si se presenta como elemento adicional, que en el direccionamiento organizacional, exista la unidad de propósito y dirección entre la controlante y la filial, caracterizada por la consecución de un objetivo común.*

*(...) La configuración de grupo empresarial podría establecerse entre una sociedad extranjera y una sola sociedad colombiana, en donde la sociedad extranjera sea dueña de más del 50% de las acciones de la sociedad colombiana, siempre y cuando se presente, adicionalmente, unidad de propósito y dirección.*

*(...) Si se configura la situación de control, esta debe revelarse mediante la inscripción en el Registro Mercantil; y si además, concurre la incorporación de Grupo Empresarial, esta situación también debe ser revelada a través de la inscripción en el Registro Mercantil, Artículo 30 de la Ley 222 de 1995 (...).”*

#### **10. SOBRE LA CAPACIDAD DE UBER COLOMBIA S.A.S. PARA CUMPLIR LAS ÓRDENES IMPARTIDAS**

Según el recurso bajo estudio, Uber Colombia S.A.S. no tiene la capacidad para cumplir las órdenes impartidas porque no tiene ningún control sobre los Datos personales de los usuarios de la plataforma. Además, su objeto social se limita a brindar servicios relacionados con soporte de ventas para publicidad, *marketing*.

Como se expuso, Uber Colombia S.A.S. puede que no tenga control absoluto sobre los Datos personales de los usuarios de la Plataforma. No obstante, esa no es razón suficiente para desatender sus responsabilidades constitucionales y legales frente al Tratamiento de los Datos personales de los usuarios de la plataforma en territorio colombiano.

La sociedad recurrente es el foco principal del Grupo Uber en Colombia, desde un punto de vista jurídico y económico. Asimismo, es corresponsable del Tratamiento de los Datos personales de los usuarios de la plataforma en Colombia, pues participa en esa actividad. Vale la pena anotar y resaltar que el Tratamiento de Datos personales no se limita

*Por la cual se resuelve un recurso de apelación*

únicamente a la recolección de los mismos, sino que comprende su uso, circulación, explotación económica, análisis y cualquier otra actividad.

Es pertinente recordar que, decidir sobre el Tratamiento de Datos personales, en cierto grado, no implica un control absoluto sobre los mismos, ni un traslado de su titularidad; pero, tampoco excluye la responsabilidad que recae sobre la sociedad en virtud de las cargas impuestas por la Constitución Política Nacional y la Ley 1581 de 2012.

Ahora, sobre la falta de capacidades legales para cumplir las órdenes impuestas en la acto administrativo recurrido, es necesario precisar que las facultades legales que tiene esta superintendencia en virtud del artículo 21 de la Ley 1581 de 2012, para impartir órdenes/instrucciones, no depende del objeto social de los destinatarios. Por tal razón, esta autoridad no puede condicionar, ni mucho menos obviar sus facultades legales al hecho de que la destinataria de las órdenes y/o instrucciones prevea -eventualmente- en su objeto social la ejecución de las mismas. Además, la recurrente debe desconocer el siguiente mandato del artículo 4 de la Constitución Política de Colombia: *“Es deber de los nacionales y de los extranjeros en Colombia acatar la Constitución y las leyes, y respetar y obedecer a las autoridades”*

En otro orden de ideas, es lógico que el cumplimiento de las órdenes impartidas en la Resolución No. 21478 de 17 de junio de 2019 es en conjunto con las demás destinatarias de las órdenes, entre las que se encuentra la Responsable principal del Tratamiento.

El cumplimiento de las órdenes por parte de Uber Colombia S.A.S. no es independiente, sino en conjunto con las demás compañías destinatarias de las mismas. Para esta superintendencia, la comunicación existente entre Uber Colombia S.A.S. y las demás compañías destinatarias de las órdenes impartidas, es la misma comunicación que tiene la sociedad recurrente con las demás compañías del Grupo Uber para cumplir su objeto social y ejecutar sus políticas comerciales.

En este punto es necesario recordar que la Resolución No. 21478 de 17 de junio de 2019 busca prevenir el daño o riesgo a los Derechos Fundamentales protegidos por la Ley 1581 de 2012. Esa finalidad tiene como fundamento el artículo 2 de la Constitución Política Nacional:

*“Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución (...) **Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades (...)**”.*

Asimismo, se soporta en las funciones que le otorgan:

- i. Los artículos 19 y 21 de la Ley 1581 de 2012;
- ii. El principio de eficacia, consagrado en los artículos 2 y 209 superiores; y
- iii. El numeral 11 del artículo 3 de la Ley 1437 de 2011.

Se aclara que, si se aceptaran los argumentos expuestos en este recurso, no habría aplicación real de la Ley 1581 de 2012 y, sería inane la existencia de la misma y de las funciones que se otorgan a esta entidad.

Por la cual se resuelve un recurso de apelación

Lo anterior también concuerda con el análisis que hizo la Corte Constitucional en la Sentencia C-748 de 2011 sobre el Principio de Seguridad. Para la cual, la Ley 1581 de 2012 se aplica en su totalidad a este tipo de plataformas. Sobre todo, cuando estamos hablando de las medidas de seguridad de la información personal:

**“2.6.5.2.7. (...) De este principio se deriva entonces la responsabilidad que recae en el administrador del dato. El afianzamiento del principio de responsabilidad ha sido una de las preocupaciones actuales de la comunidad internacional, en razón del efecto “diluvio de datos [sic]”, a través del cual [sic] día a día la masa de datos [sic] personales existente, objeto de tratamiento [sic] y de ulterior transferencias, no cesa de aumentar. Los avances tecnológicos han producido un crecimiento de los sistemas de información, ya no se encuentran sólo [sic] sencillas bases [sic] de datos [sic], sino que surgen nuevos fenómenos como las redes sociales, el comercio a través de la red, la prestación de servicios, entre muchos otros. Ello también aumenta los riesgos [sic] de filtración de datos [sic], que hacen necesarias la adopción de medidas eficaces para su conservación. Por otro lado, el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre.**

**En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, por ejemplo, en materia de redes sociales, empieza a presentarse una [sic] preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. En el año 2009, el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea señaló que en los Servicios de Redes Sociales” o “SRS debe protegerse la información del perfil en el usuario mediante el establecimiento de “parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos”<sup>12</sup>. (Destacamos).**

## 11. SEGURIDAD Y CONFIANZA

Sin seguridad no hay debido tratamiento de datos personales. Por eso, la Ley 1581 de 2012 establece lo siguiente: *“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; (...)”<sup>13</sup>*

En desarrollo de lo anterior, la Ley impone a los Responsables y Encargados del Tratamiento los siguientes deberes:

- *“Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; (...)”<sup>14</sup>*
- *“Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares”*

<sup>12</sup> Corte Constitucional, Sentencia C-748 de 2011, 6 de octubre de 2011, Magistrado Ponente Jorge Ignacio Pretelt, Considerando 2.6.5.2.7.

<sup>13</sup> Cfr. Literal g) del artículo 4 de la Ley 1581 de 2012

<sup>14</sup> Cfr. Literales d) y b) de los artículos 17 y 18 de la Ley 1581 de 2012

*Por la cual se resuelve un recurso de apelación*

El principio y el deber de seguridad tiene un criterio eminentemente preventivo, lo cual obliga a los Responsables o Encargados del Tratamiento a adoptar las medidas necesarias para evitar posibles afectaciones a la seguridad de los datos. Pero, si las medidas de seguridad fallan, las organizaciones deben estar preparadas para mitigar los riesgos y daños que se pueden causar a los derechos y las libertades fundamentales de los Titulares y a las organizaciones, los cuales pueden ser de gravedad y probabilidad variables, materiales o inmateriales.

La seguridad es un tema complejo que dicta buena parte de lo que debe ser un tratamiento debido de datos personales *-desde la recolección, su uso, almacenamiento, análisis, circulación y cualquier otra actividad-*.

La seguridad requiere un enfoque multidisciplinar *-incluye a ingenieros, físicos, matemáticos, administradores, abogados, entre otras especialidades-* y abarca muchos enfoques desde el tecnológico, pasando por lo jurídico, físico, administrativo administrativo hasta lo humano.

La seguridad impacta en muchas áreas y sectores de relevancia social y económica. Al tratarse de un asunto estratégico para el tratamiento de datos personales, resulta necesario que las empresas no ahorren esfuerzos en garantizarla en todo momento y en actuar de oficio *-no por orden de las autoridades-* para generar confianza en sus clientes y en la sociedad. Es necesario que los procesos de seguridad no se queden pactados en los documentos sino que sea implementados en la práctica. No basta la “seguridad en el papel” sino en la realidad de las operaciones y en las prácticas de una organización.

No se trata únicamente de redactar textos o políticas sino de aplicar en la práctica todo lo que se dice o promete en las políticas, publicidad y demás comunicaciones de los Responsables o Encargados.

No se ajusta a derecho ni es ético prometer seguridad en el papel y no cumplirla o garantizarla en el día día de las operaciones o actividades de una empresa. El desafío de la seguridad es inmenso. Es imprescindible asegurar permanentemente los datos personales *-No ocasionalmente-*.

Desde hace algunas décadas se ha afirmado que la confianza es factor crucial para el crecimiento y consolidación de cualquier actividad que involucre el tratamiento de datos personales. Por eso, se ha sostenido que *“las actividades continuas de creación de confianza deben ser una de las prioridades estratégicas más importantes para cada organización”*<sup>15</sup>.

La confianza se entiende como la expectativa de que *“se puede contar con la palabra del otro”*, y de que se emprenderán acciones positivas y beneficiosas entre las partes de manera recíproca. Cuando existe confianza, la persona cree que una entidad es fiable; cumple su palabra; es sincera; íntegra y lleva a cabo con las acciones prometidas<sup>16</sup>.

La seguridad genera confianza. Si falla, es clave estar muy bien preparados y entrenados para actuar frente a los incidentes de manera inmediata, profesional e inteligente. Parte de la confianza de una organización también depende del cumplimiento de la ley y de las órdenes preventivas de las autoridades para evitar causar daños a sus clientes.

<sup>15</sup> Cfr. Edelman Trust Barometer de 2019. <https://www.edelman.com/trust-barometer>

<sup>16</sup> Cfr. Barrera Duque, Ernesto (2018) *Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales*. Universidad de la Sabana y Ecoe ediciones.

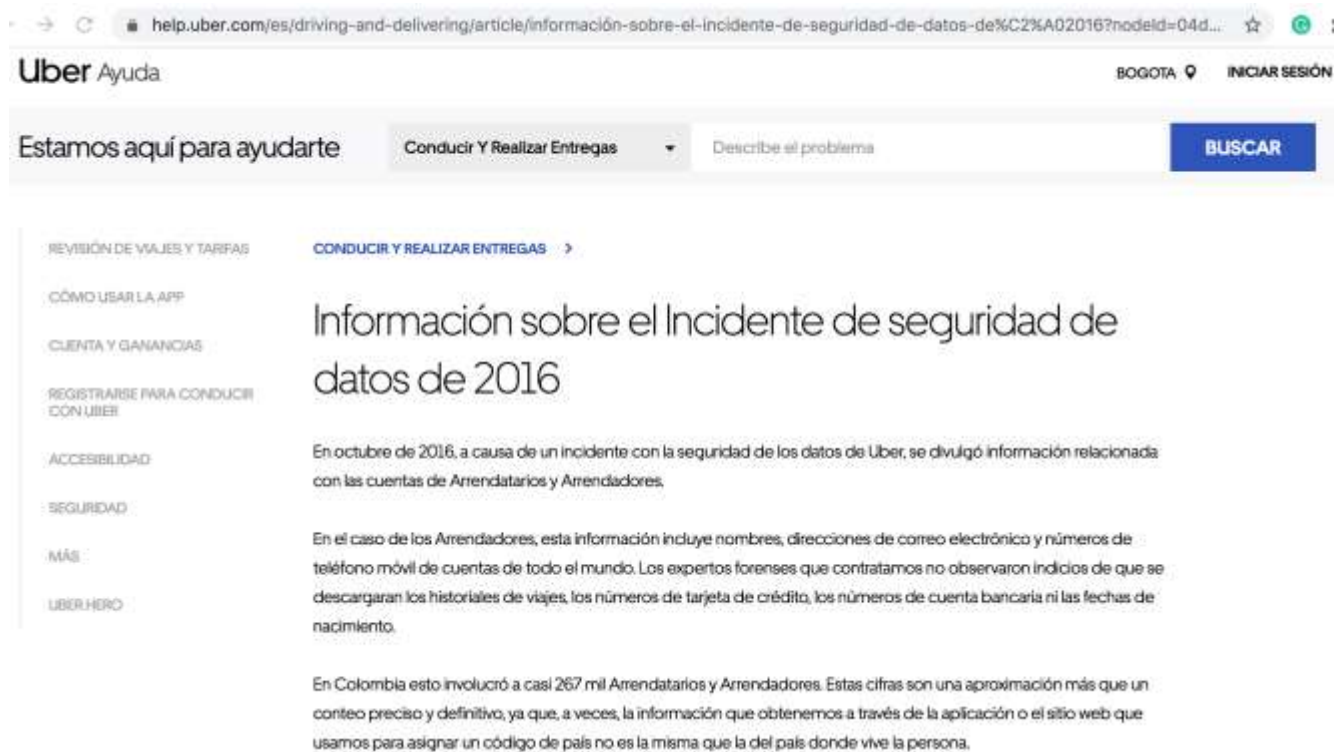
Por la cual se resuelve un recurso de apelación

VERSIÓN PÚBLICA

## 12. DETECCIÓN DE INCIDENTES DE SEGURIDAD Y PROTOCOLOS DE RESPUESTA

El incidente de seguridad ocurrido y que dio origen a la orden de esta entidad a UBER, afectó a un estimado de 267.000 usuarios colombianos, tal como se dio a conocer en la primera instancia de esta actuación administrativa y fue reconocido por UBER.

Lo anterior se puede constatar en la siguiente imagen de la nota publicada por UBER<sup>17</sup>



Como se menciona, las medidas de seguridad tienen un carácter preventivo para evitar la pérdida de la información, su adulteración, así como la consulta, uso, circulación o acceso no autorizado o fraudulento.

Las medidas de seguridad deben ser apropiadas considerando varios factores como: (i) los niveles de riesgo del Tratamiento para los derechos y libertades de los Titulares de los datos; (ii) la naturaleza de los datos; (iii) las posibles consecuencias que se derivarían de una vulneración para los Titulares, y la magnitud del daño que se puede causar a ellos, al Responsable y a la sociedad en general; (iv) el número de Titulares de los datos y la cantidad de información; (v) el tamaño de la organización; (vi) los recursos disponibles, (vii) el estado de la técnica, y (viii) el alcance, contexto y finalidades del Tratamiento de la información.

Todas las medidas de seguridad, deben ser objeto de revisión, evaluación y mejora permanente.

Ahora bien, si la seguridad falla, es fundamental que las organizaciones cuenten con mecanismos de monitoreo y control que les permita detectar de inmediato o prontamente el incidente de seguridad. Esto ayudará reducir la magnitud del daño para la organización y para los Titulares de la Datos Personales. Por ende, es crucial que se cuente con herramientas de “alertas” para actuar tan pronto ocurra el incidente.

<sup>17</sup> CFR. <https://help.uber.com/es/driving-and-delivering/article/informaci%C3%B3n-sobre-el-incidente-de-seguridad-de-datos-de-%C2%A02016?nodeId=04d4d787-ca99-40a3-ab27-9af42d196575> . Última consulta: 28 de septiembre de 2020

*Por la cual se resuelve un recurso de apelación*

Las organizaciones deben aplicar todas las medidas técnicas, administrativas y organizativas para determinar de inmediato si se ha producido un incidente de seguridad que afecte los datos personales y, de ser así, tienen que implementar las acciones necesarias para abordar dicho evento u ocurrencia. Así mismo, en cumplimiento de lo que establece la Ley 1581 de 2012, reportarlo a la SIC y, dependiendo del caso, comunicarlo a los Titulares de la Información.

Todos los incidentes de seguridad deben ser tomados seriamente y evaluados por parte de las organizaciones. Los que inicialmente parezcan irrelevantes podrían ser significativos o graves respecto de los los derechos y las libertades de los Titulares de la información.

Es crucial que las organizaciones entrenen periódicamente a su equipo humano para actuar frente al incidente. Se recomienda efectuar simulacros preventivos como se hacen, por ejemplo, para casos de incendios o temblores. Frente a un incidente, la gente debe estar preparada para actuar de inmediato, profesionalmente e inteligentemente.

Finalmente, las organizaciones deben contar con un protocolo de respuesta en el manejo de incidentes que comprenda los roles, responsabilidades y acciones que deben ser desplegadas al interior de las organizaciones para gestionar un incidente de seguridad. Dicho instrumento debe ser:

- Documentado.
- Implementado
- Comunicado al equipo humano de la organización.
- Monitoreado.

El monitoreo consiste en realizar un seguimiento constante para velar porque las medidas que se hayan establecido al interior de las organizaciones se apliquen y funcionen en la práctica.

### **13. CIBERSEGURIDAD**

Una empresa como Uber, 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 UBER.

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”*<sup>18</sup> y a *“conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”*<sup>19</sup>. Sino que, 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”*<sup>20</sup>.

Uber 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**

<sup>18</sup> Cfr. Literal g) del artículo 4 de la Ley Estatutaria 1581 de 2012

<sup>19</sup> Cfr. Literal d) del artículo 17 de la Ley Estatutaria 1581 de 2012

<sup>20</sup> Cfr. Artículo 26 del decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015)

*Por la cual se resuelve un recurso de apelación*

### **recursos ni voluntad para responder por la seguridad de los datos de miles de millones de personas.**

Se recalca 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 otros, los hechos; investigaciones; actuaciones y conclusiones de Autoridades de Protección de Datos, que tienen como objetivo que Uber: (i) asuma la responsabilidad por las fallas de seguridad y la exposición de la información personal de sus usuarios; y (ii) desarrolle nuevos protocolos que protejan, de manera efectiva, los Datos de sus usuarios para asegurar que un evento como el sucedido no ocurra nuevamente.

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 Uber para garantizar en la práctica, la seguridad de los Datos personales y de los ciudadanos usuarios de esa plataforma de servicios.

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

#### **14. LAS ÓRDENES NO SON SANCIONES**

Una orden administrativa no es una sanción, sino una medida necesaria para la adecuación de las actividades u operaciones de los Responsables del Tratamiento a las disposiciones de la regulación colombiana sobre protección de datos personales. 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.

Para garantizar el debido tratamiento de los Datos se consideró necesario impartir la orden recurrida por UBER.

#### **15. CONCLUSIONES**

Sin perjuicio de lo establecido, no se accederá a las pretensiones de Uber Colombia S.A.S. ni Uber B.V. por las siguientes razones:

1. La Ley 1581 de 2012 es aplicable a UBER B.V. 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.
2. La seguridad es un tema que no solo afecta a los Titulares de los Datos, sino a los intereses de las empresas porque de ello depende la protección de sus activos, su reputación, su buen nombre y la confianza que genera en el mercado, el ciberespacio y en los diferentes países en donde efectúa actividades de recolección y uso de datos personales. La seguridad es esencial para garantizar el debido tratamiento de los datos de los clientes, empleados y terceros.
3. Mediante un comunicado de Dara Khosrowshahi (Chief Executive Officer de Uber), se informó que "(...) a finales de 2016 dos individuos ajenos a la Compañía obtuvieron de forma inapropiada acceso a datos de usuarios almacenados en un servidor en la nube alojado por un proveedor externo que utilizábamos". Ese incidente de seguridad

*Por la cual se resuelve un recurso de apelación*

- afectó a un estimado de 267.000 usuarios colombianos, tal como se dio a conocer en la primera instancia de esta actuación administrativa y fue reconocido por UBER<sup>21</sup>.
4. 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 Uber.
  5. Esta superintendencia sí tiene competencia para imponer las órdenes contenidas en la Resolución No. 21478 de 17 de junio de 2019 tal y como se puede evidenciar en el literal e) del artículo 21 de la Ley Estatutaria 1581 de 2012;
  6. En el desarrollo de la actuación administrativa que terminó con la expedición de la Resolución No. 21478 de 17 de junio de 2019 se respetaron todas las garantías procesales, constitucionales y legales, y los Derechos Fundamentales de la recurrente;
  7. El procedimiento seguido para emitir la Resolución No. 21478 de 17 de junio de 2019 es el previsto en la ley para este tipo de actuaciones;
  8. En ningún momento esta superintendencia desestimó la personalidad jurídica de ninguna de las compañías del Grupo Uber;
  9. Las formalidades o apariencias jurídicas de ese diseño no priman sobre la notoria realidad material.

Tratándose de la protección de Derechos Humanos Fundamentales, se deben desestimar las formas y las apariencias, e imponer la materialidad de lo que sucede en la práctica para garantizar la efectividad de los mismos. Y, cumplir el mandato constitucional del artículo 15 según el cual, *“En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución”*. Disposición suprema reglamentada por la Ley Estatutaria 1581 de 2012, la cual exige que los datos personales se traten con *“las 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”*<sup>22</sup>

Téngase presente que la *“Constitución es norma de normas”*<sup>23</sup> y que *“en todo caso de incompatibilidad entre la Constitución y la ley u otra norma jurídica, se aplicarán las disposiciones constitucionales”*<sup>24</sup>. Adicionalmente, *“es deber de los nacionales y de los extranjeros en Colombia acatar la Constitución y las leyes, y respetar y obedecer a las autoridades”*<sup>25</sup>;

10. **Uber Colombia S.A.S. realiza una actividad que involucra el Tratamiento de Datos personales. Pues, para prestar sus servicios de publicidad utiliza los Datos de los usuarios de Uber Sin esta información, esa sociedad colombiana no podría prestar sus servicios.**  
**En otras palabras, el modelo de negocios de Uber Colombia S.A.S. se basa en la recolección, uso y circulación de la información que realiza Uber.**
11. Uber Colombia S.A.S. tiene un rol fundamental en el Tratamiento de Datos personales para la prestación de servicios, apoyo en ventas de publicidad y mercadeo;
12. Uber Colombia S.A.S. es corresponsable del Tratamiento de Datos personales de los usuarios de la plataforma en Colombia, en virtud de sus vínculos jurídicos y económicos con el Uber y su participación en el Tratamiento de esos Datos;

<sup>21</sup> CFR. <https://help.uber.com/es/driving-and-delivering/article/informaci%C3%B3n-sobre-el-incidente-de-seguridad-de-datos-de-%C2%A02016?nodeId=04d4d787-ca99-40a3-ab27-9af42d196575> . Última consulta: 28 de septiembre de 2020

<sup>22</sup> Cfr. Literal g) del artículo 4 de la Ley Estatutaria 1581 de 2012

<sup>23</sup> Cfr. Artículo 4 de la Constitución de la República de Colombia

<sup>24</sup> Loc. cit.

<sup>25</sup> Loc. cit.



VERSIÓN PÚBLICA

*Por la cual se resuelve un recurso de apelación*

13. **Uber Colombia S.A.S.**, tiene la obligación y capacidad -en conjunto con **UBER TECHNOLOGIES, INC.**, y **UBER B.V.**-, para dar cumplimiento a las órdenes impartidas en la Resolución No. 21478 de 17 de junio de 2019;
14. Las sociedades objeto de las órdenes impuestas 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. 21478 de 17 de junio de 2019;
15. Una empresa como Uber, 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 UBER.

**Sin seguridad no hay debido tratamiento de datos personales. Así las cosas, Uber debe ser responsable, diligente y muy profesional con el tratamiento seguro de los datos personales.**

En mérito de lo expuesto, este Despacho,

**RESUELVE**

**PRIMERO.** Confirmar en todas sus partes la Resolución No. 21478 de 17 de junio de 2019, ratificada mediante la Resolución No. 47593 del 18 de agosto de 2020, por las razones expuestas en la parte motiva de este acto administrativo.

**SEGUNDO.** Notificar personalmente el contenido de la presente resolución a las sociedades: **LIEBER COLOMBIA S.A.S.**, identificada con Nit. 900.676.165-2, **UBER MANAGEMENT B.V.**, identificada con Nit. 900.972.019-4; y, **UBER B.V.** con Registro Comercial No.56317441 a través de sus representantes legales o apoderados, entregándoles copia de la misma.

**NOTIFÍQUESE Y CÚMPLASE**

Dada en Bogotá, D.C., 28 de septiembre de 2020

**El Superintendente Delegado para la Protección de Datos Personales,**

**NELSON REMOLINA ANGARITA**

Por la cual se resuelve un recurso de apelación

VERSIÓN PÚBLICA

## Notificación

### Investigado

Sociedad: **LIEBER COLOMBIA S.A.S.**  
Identificación: Nit. 900.676.165-2  
Representante legal: **UBER MANAGEMENT B.V.**  
Identificación: Nit. 900.972.019-4  
Dirección: Carrera 14 No. 93-68 Piso 5, Edificio Corteza 93  
Correo electrónico: [colombianotifica@uber.com](mailto:colombianotifica@uber.com)  
Apoderada: [REDACTED]  
Identificación: [REDACTED]  
Tarjeta Profesional: [REDACTED]  
Dirección: [REDACTED]  
Ciudad: [REDACTED]  
Correo electrónico: [REDACTED]

Sociedad: **UBER B.V.**  
Identificación: Registro Comercial 56317441  
Dirección: Mr. Treublaan 7, 1097 DP  
Ciudad: **ÁMSTERDAM**  
País: Países Bajos  
Representante legal: [REDACTED]  
Identificación: [REDACTED]  
Tarjeta Profesional: [REDACTED]  
Dirección: [REDACTED]  
Ciudad: [REDACTED]  
Correo electrónico: [REDACTED]