REPÚBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 83381 DE 2021

(Diciembre 23 de 2021)

Por la cual se resuelve un recurso de apelación

Radicado 20-87350

VERSIÓN ÚNICA

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, numeral 7 del artículo 16 del Decreto 4886 de 2011, y

CONSIDERANDO

PRIMERO. Que, mediante la Resolución No. 74519 del 23 de noviembre de 2020, la Dirección de Investigación de Protección de Datos Personales de la Superintendencia de Industria y Comercio con el fin de garantizar el debido Tratamiento de Datos personales en el territorio colombiano emitió las siguientes órdenes administrativas de carácter preventivo a la sociedad ZOOM VIDEO COMMUNICATIONS, INC:

*"**ARTÍCULO PRIMERO.** ORDENAR a la sociedad ZOOM VIDEO COMMUNICATIONS, INC en adelante Zoom, 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 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 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 Zoom;
c) La naturaleza y el ámbito de las actividades de Zoom;
d) La cantidad de Titulares;
e) La naturaleza de los Datos personales;
f) El tipo de Tratamiento de los Datos personales;
g) El alcance, contexto y fines del Tratamiento;

h) Las actualizaciones o cualquier tipo de modificación de la plataforma de Zoom, sus productos y cualquier otra forma en que Zoom utilice, recopile, comparta o trate los datos recolectados;
i) El acceso a los Datos personales por parte de los empleados, contratistas y en general los colaboradores de Zoom;
j) El uso de los Datos personales de los usuarios por terceros, entre ellos, aliados
comerciales, empresas asociadas y desarrolladores de aplicaciones, si aplica;
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 personales; y
m) Los riesgos para los derechos y libertades de los Titulares.

3) Desarrollar, implementar y mantener un programa de gestión y manejo de incidentes de seguridad en Datos personales, que contemple procedimiento para información sin dilación indebida a esta Superintendencia de Industria y Comercio y a los Titulares de los mismos cuando se presenten incidentes que afecten la confidencialidad, integridad y disponibilidad de los Datos 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 personales y su política de Tratamiento de Datos personales (o privacidad) de Zoom.

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)Zoom 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, certificar a esta entidad que cuenta con las medidas técnicas, humanas, administrativas, contractuales y de cualquier otra naturaleza que sean necesarias para otorgar seguridad a los Datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."

ARTÍCULO SEGUNDO. *La sociedad ZOOM VIDEO COMMUNICATIONS, INC deberá cumplir lo ordenado en esta resolución dentro de los cuatro (4) meses siguientes a la ejecutoria del presente acto administrativo y acreditar ante la Dirección de Investigaciones de Protección de Datos Personales de la Superintendencia de Industria y Comercio las medidas y procedimientos adoptados dentro de los cinco (5) días siguientes al vencimiento de dicho término.*

PARÁGRAFO PRIMERO. *Para demostrar el cumplimiento, la sociedad ZOOM VIDEO COMMUNICATIONS, INC deberá 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 deber de seguridad de la Ley Estatutaria 1581 de 2012 respecto de los Datos personales.

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

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

SEGUNDO. Que, mediante comunicación 20-873550-10, de 10 diciembre de 2020, ZOOM VIDEO COMMUNICATIONS, INC (en adelante, la recurrente o Zoom), a través de apoderado, presentó recurso de reposición y en subsidio apelación contra la Resolución No. 74519 del 23 de noviembre de 2020, en el que, entre otras consideraciones, manifestó lo siguiente:

"En este caso, para la fecha de la presentación de este documento, Zoom no ha recibido aún una notificación oficial de la Resolución, por lo tanto, la presentación del presente recurso es oportuna."

TERCERO. Que, mediante comunicación 20-87350- 17 de 22 de enero de 2021, la recurrente, a través de apoderado, presentó escrito con asunto "*Memorial sobre la indebida notificación a Zoom*", en el que solicita lo siguiente:

"*Modificar o revocar la "Certificación/Informe Notificación" registrado en el portal de la SIC el 20 de enero de 2020 y suscrito por el COORDINADOR GRUPO NOTIFICACIONES Y CERTIFICACIONES en donde se declara que la notificación de la Resolución 74519 de 2020 fue surtida el 13 de enero de 2020, de manera que (i) se surtan las notificaciones respectivas de manera correcta a través de los canales indicados por Zoom, o (ii) se declare que la fecha de notificación que no podrá ser anterior al 21 de enero de 2021, por cuanto solo hasta fecha la SIC habilitó al apoderado de Zoom el acceso al expediente de la referencia*."

CUARTO. Que, mediante escrito 20-87350-19 de 27 de enero de 2021, la recurrente presentó, en una segunda oportunidad, recurso de reposición y en subsidio apelación contra la Resolución No. 74519 del 23 de noviembre de 2020, con fundamento en los siguientes hechos y argumentos:

i. Declaración preliminar:

- Indica que: "*Zoom radicó previamente una versión de este recurso el 10 de diciembre de 2020. Zoom está radicando nuevamente este recurso con ajustes en respuesta a la supuesta notificación por parte de la SIC el 13 de enero de 2021 y basado en la*

revisión por parte de Zoom de los archivos del expediente, a los cuales no tuvo acceso sino hasta el 21 de enero de 2021. (…)"[1]

- Manifiesta que "*Zoom respondió al requerimiento del 13 de abril de 2020 de la SIC sobre las prácticas de seguridad de Zoom (el "Requerimiento"), presentando su respuesta del 13 de mayo de 2020 (la "Respuesta"), en la que contestó a las preguntas de la SIC y confirmó que los datos personales de ningún ciudadano colombiano fueron expuestos o comprometidos debido a las acciones u omisiones de Zoom, manteniendo al mismo tiempo la postura de Zoom de que no está sujeta a la jurisdicción de Colombia. Sin hacer preguntas complementarias, ni brindarle a Zoom ninguna posibilidad de responder a las preocupaciones de la SIC, la SIC emitió la Resolución N.° 74519 de 2020, de fecha 23 de noviembre de 2020 en la que se obliga a Zoom a establecer una estrategia de mejora de su seguridad."*[2]

ii. Presentación oportuna del recurso:

- Señala que, según el artículo 76 de la Ley 1437 de 2011: "*una persona tendrá 10 días hábiles después de ser notificada de una decisión emitida por una entidad administrativa para presentar los recursos de reposición y de apelación. Conforme a la información disponible en el portal de Servicios en Línea de la SIC (el "PSL"), la SIC considera que Zoom fue notificada de la Resolución 74519 de 2020 el 13 de enero de 2021. (…) Zoom presenta este recurso de reposición y en subsidio apelación para proteger su derecho a la defensa, así como hizo al presentar la versión anterior de este recurso el 10 de diciembre de 2020*."[3] Lo anterior, indica, sin perjuicio de lo dicho mediante comunicación 20-87350- 17 de 22 de enero de 2021.

iii. La SIC no tiene jurisdicción sobre Zoom

Lo anterior, por los siguientes motivos:

- "***La SIC carece de autoridad para regular las actividades de Zoom fuera de Colombia***":

  (i) "*El RPDC no se aplica a Zoom y la Resolución es nula porque Zoom, como empresa extranjera, no realiza operaciones de procesamiento de datos personales dentro del territorio colombiano: (…) la SIC no identifica, ni en la Resolución ni en el Análisis Técnico ningún evento en que datos personales pertenecientes a ciudadanos colombianos hayan sido expuestos o comprometidos debido a las actividades de tratamiento de Zoom, ya sea dentro o fuera del territorio colombiano*"[4]

  (ii) "*El RPDC rige únicamente para el procesamiento de datos realizado dentro de Colombia, o según lo permita un tratado internacional (La Resolución no cita ninguno, porque no hay tratado aplicable)" -Art 2 de la Ley 1581 de 2012-*[5] *(…) "la sentencia C-748 de 2011 no permite a la SIC ejercer jurisdicción sobre el tratamiento de datos de*

[1] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 1, pie de página No. 1.
[2] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 1.
[3] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 3.
[4] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 4.
[5] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 4.

Zoom fuera de Colombia (salvo que un tratado internacional lo permitiera, lo cual no es así)."[6]

(iii) "*La propia SIC, en respuesta a un derecho de petición confirmó que el RPDC no le permitía regular el tratamiento de datos por parte de Facebook a través de Internet, porque "dicha compañía en la actualidad no tiene domicilio en Colombia*" -Consulta Pública No. 14-218349-3 (2014)-[7]

(iv) "*El alcance limitado de la Ley colombiana es compatible con el artículo 4 de la Constitución colombiana, que deja claro que el derecho colombiano rige para los "nacionales y [...] los extranjeros en Colombia". Zoom no ha establecido una presencia local en Colombia que lo someta al derecho colombiano. Zoom ya ha explicado a la SIC que no tiene ninguna filial, sucursal o subsidiaria en Colombia, y que no mantiene servidores para el almacenamiento o procesamiento de datos personales o de información dentro del territorio colombiano, así como tampoco proveedores de servicios de almacenamiento de información y datos*"[8] Por lo anterior, reafirma que *"la Ley 1581 de 2012, no permite que la SIC regule las operaciones de tratamiento de datos de Zoom en el extranjero"*[9]

(v) "*El intento de la SIC por ejercer jurisdicción sobre Zoom también es contrario al principio de soberanía nacional. La Corte Constitucional de Colombia - T-462 de 2015- ha reconocido que las naciones solo tienen poder para regular las acciones que ocurren en sus territorios (o cuando el Estado en el que la entidad extranjera tiene su sede ha dado su consentimiento para limitar su propia soberanía, lo cual no es el caso aquí). Zoom tiene su sede en los Estados Unidos de América, y no tiene presencia local en Colombia. Por tanto, sería contrario al principio de soberanía nacional por parte Colombia intentar aplicar sus propias leyes a Zoom."*[10]

Concluye la recurrente que:

"*Debido a que el RPDC rige solo para los responsables o encargados que se establecen por sí mismos y llevan a cabo actividades de procesamiento de datos en Colombia, y debido a que Zoom no es un responsable o encargado de este tipo, la SIC no puede ejercer jurisdicción sobre Zoom para regular sus operaciones en los Estados Unidos de América*"[11]

- "***El uso de cookies por parte de Zoom no establece jurisdicción***":

(i) *"(…) El intento de la SIC de ejercer jurisdicción sobre Zoom basado en el uso de cookies es contrario al derecho colombiano. (…) la Resolución no aclara en qué tipo de cookies se basa para reclamar la jurisdicción, ni especifica los datos personales supuestamente tratados por Zoom a través de estas cookies. (…) La legislación colombiana no regula explícitamente las cookies, a diferencia, por ejemplo, de la Unión Europea, donde la Directiva de Privacidad Electrónica (...) regula el uso de ciertos tipos de cookies según cómo son utilizadas y dependiendo si a través de ellas se procesan ciertos tipos de datos*"[12]

---

[6] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág.5.
[7] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 4.
[8] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, págs. 4 y 5.
[9] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 5.
[10] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 5.
[11] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 5.
[12] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 5.
[12] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 6.

(ii) "*La SIC ha reconocido que la situación jurídica de las cookies conforme a la legislación colombiana no es clara, y únicamente afirma que puede "eventualmente" determinarse que las cookies puedan, en determinados contextos fácticos, tratar datos personales - Respuesta Derecho de Petición radicado No. 16-172268-1 (2016)-"*[13]

(iii) "*La SIC no puede invocar las cookies utilizadas para soportar la operación de un sitio web disponible de manera generalizada como fundamento para regular las actividades extraterritoriales de una empresa extranjera. El sitio web de Zoom está disponible en todo el mundo: Zoom no tiene un sitio web específico de Colombia ni campañas de marketing específicas para Colombia. Zoom no hace esfuerzos específicos para orientar las cookies de su sitio web a los usuarios de Colombia. Y, como se señaló anteriormente, Zoom no tiene oficina física, filial local u otras actividades de procesamiento de datos en Colombia (...)"*[14]

(iv) "*La afirmación de la SIC de que el uso de cookies permite el ejercicio de la jurisdicción permitiría a la SIC eludir las limitaciones jurisdiccionales del artículo 2 de la Ley 1581 de 2012 con respecto a cualquier empresa cuyo sitio web es accesible dentro de Colombia, esencialmente, todas las empresas del mundo. Este es un argumento insostenible, incompatible con la clara intención del Congreso de que la Ley 1581 de 2012 se aplique únicamente a las actividades de tratamiento de datos que ocurren dentro del territorio colombiano."*[15]

(v) "Los tribunales colombianos han declarado específicamente que los fallos emitidos por autoridades extranjeras en materia de protección de datos no son vinculantes en Colombia -T-277 de 2015-. La Resolución se basa en la decisión de 2013 de la AEPD- Agencia Española de Protección de Datos- contra Google (...) sin reconocer la gran disparidad entre el marco de protección de datos español y colombiano, y las cuestiones de hecho que motivaron la Decisión de la AEPD".[16]

iv. La resolución es nula por ausencia del debido proceso, falta de pruebas y análisis jurídico.

Justifica lo anterior en los siguientes argumentos:

- **Zoom no tuvo una oportunidad justa de ejercer su defensa**:

(i) "*(…) La SIC llegó a sus conclusiones sin darle a Zoom una oportunidad adecuada para presentar una defensa. Por consiguiente, la resolución carece de sustento jurídico y fáctico en sus consideraciones*."[17]

(ii) "*Zoom no tuvo la oportunidad adecuada de contradecir las pruebas invocadas por la SIC en la Resolución. El Requerimiento no citó el artículo de "Bleeping Computer", el artículo de "Hacker News", el artículo de "Vice" o el artículo de "New York Times", en los que ahora se basa la Resolución. Esos documentos no fueron revelados sino en la resolución misma, lo que significa que Zoom no tuvo oportunidad de responder*

[13] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 6.
[14] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 6.
[15] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, págs. 6 y 7.
[16] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 7.
[17] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 8.

a ellos y de explicar las razones por las cuales su contenido no describe con precisión la seguridad de Zoom (…)

La SIC tampoco le dio a Zoom la oportunidad de explicar su uso de cookies antes de utilizar ese argumento como fundamento para su jurisdicción (…)

(iii) *(L)a Resolución se basa en gran medida en el anuncio de la FTC de la propuesta de acuerdo voluntario con Zoom, que se anunció a principios de noviembre, y sobre el cual la SIC no hizo ninguna pregunta a Zoom. (…)*

Este principio fundamental del debido proceso debe preservarse incluso cuando la decisión adoptada por una autoridad no sea una sanción, sino simplemente una orden administrativa sin una sanción económica explícita (pero con consecuencias económicas potencialmente materiales). (…) En este caso, es claro que la Resolución impone cargas indebidas a Zoom y no le permitió presentar una defensa adecuada de manera previa."[18]

Frente al particular, concluye la recurrente lo siguiente:

"*Estas omisiones por parte de la SIC constituyen una violación del derecho a la defensa de Zoom, que a su vez es una violación del debido proceso en el procedimiento administrativo, ya que la SIC no permitió que Zoom presentara ninguna defensa, consideración o argumento previo sobre las evidencias citadas por la SIC como fundamento de la Resolución*."[19]

- **La resolución no se basa en pruebas adecuadas ni en un análisis jurídico:**

(i) "*La SIC ha ignorado (o no ha ofrecido a Zoom una oportunidad justa para probar) que la seguridad de Zoom sería adecuada conforme al RPDC, y la SIC no ha podido establecer ningún hecho que respalde su conclusión de que la seguridad de Zoom es inadecuada*."[20] "*La SIC no tuvo en cuenta las medidas de seguridad actuales de Zoom ni probó que se hayan violado, no presentó ninguna prueba sobre las prácticas de seguridad de Zoom (invocando solo un puñado de artículos de noticias, más una queja presentada por la FTC), y no presentó ningún sustento jurídico que respaldara su imposición de cargas regulatorias onerosas a Zoom*"[21]

(ii) *"(L)a mera mención de que "aún subsisten algunas falencias" no constituye un análisis jurídico suficiente para justificar las onerosas obligaciones de cumplimiento establecidas en la Resolución, en particular porque todas las acusaciones de los artículos de noticias y la queja de la FTC se refieren a cuestiones que, para empezar, no eran vulnerabilidades de seguridad, o bien que ya han sido atendidas por Zoom.*

(…) "(*E)l "Análisis Técnico" que fue realizado por la SIC no provee ni sustenta la afirmación por parte de la SIC en la Resolución de que "aún subsisten algunas falencias". Al contrario, el Análisis Técnico no identifica ninguna vulnerabilidad de seguridad actual, y en cambio, confirma que Zoom ha resulto los posibles problemas que fueron citados en la Resolución*" [22]

---

[18] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, págs. 8 y 9.
[19] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 9.
[20] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 9.
[21] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 8.
[22] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 9.

- **No existe evidencia reprochable de la supuesta seguridad inadecuada de Zoom (incluso si Zoom estuviera sujeto al derecho colombiano)**:

  (i) "*Ni la Resolución ni el Análisis Técnico contienen constataciones de que los datos personales de cualquier residente colombiano hayan estado alguna vez sujetos a adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*"[23]

  (ii) "*Las prácticas de seguridad de Zoom son más que suficientes para cumplir con estas normas establecidas conforme al RPDC en aquellos eventos en que Zoom actúa como responsable del tratamiento*."

  Lo anterior, en consideración de la recurrente, por los siguientes motivos:

  > "***Primero.*** *Zoom tiene un oficial que calificaría como oficial de protección de datos en virtud de la Guía para la implementación del Principio de Responsabilidad Demostrada: Lynn Haaland (…).*
  > ***Segundo.*** *Zoom ha implementado controles y procesos apropiados para garantizar la seguridad de los datos personales, lo que incluye la capacitación, la gestión de riesgos y estrategias de mitigación de incidentes de riesgo. (…)*
  > ***Tercero****. Zoom reevalúa regularmente sus prácticas y mejora su seguridad a medida que su negocio crece y a medida que se da cuenta de nuevas amenazas, como lo requeriría la Guía para la implementación del Principio de Responsabilidad Demostrada (…) Sin embargo, la SIC no tuvo en cuenta ni en el Análisis Técnico como en la Resolución, las pruebas presentadas por Zoom en su Respuesta concerniente a su seguridad, y no dio a Zoom la oportunidad de presentar las pruebas adicionales que permiten concluir que su seguridad es adecuada. Dado que los términos de la Resolución no son consistentes o complementarios a los compromisos anticipados de Zoom en el acuerdo que fue propuesto con la FTC, la Resolución impone una carga gravosa que no implicará necesariamente beneficios a los ciudadanos colombianos"*[24]

- **Artículos de noticias aislados y el Acuerdo propuesto con la FTC no sustentan la imposición de obligaciones de cumplimiento a Zoom por parte de la SIC**:

  (i) "*A la luz de esta total ausencia de evidencia de algún daño real a usuarios en Colombia, en lugar de analizar la seguridad de Zoom y evaluar su idoneidad, la Resolución recopila artículos de noticias infundados sobre especulaciones relacionadas con cuatro temas distintos, así como también la decisión voluntaria de Zoom de llegar a un acuerdo con la FTC. (...) Estas fuentes infundadas no son pruebas conducentes o pertinentes sobre las prácticas generales de seguridad sobre los datos personales tratados por Zoom, y no se enmarcan bajo el principio de inmediación previsto en la ley colombiana ni respaldan la conclusión de la SIC de que hoy "aún subsisten algunas falencias (…)*

  (ii) *La Resolución tampoco establece que los usuarios en Colombia alguna vez hayan sufrido (o enfrenten el riesgo de sufrir) algún daño (…)"*[25]

  "(...) Zoom no reconoce que ninguna de las cuestiones informadas en los artículos de noticias citados por la Resolución haya generado una "falla" de seguridad, y mucho

[23] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 8.
[24] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, págs. 10 y 11.
[25] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 12.

menos que constituyan una prueba de que las medidas de seguridad de Zoom eran insuficientes (…)"[26]

Por tanto, concluye la recurrente que:

" *En la medida en que la Resolución se basa en estos artículos de noticias, ello violaría los principios fundamentales del debido proceso, porque los informes de prensa no son pertinentes ni conducentes conforme el artículo 168 del CGP para establecer en qué medida las supuestas "fallas" realmente existían, y en qué medida dichos supuestos incidentes contradicen el hecho claro de que Zoom ha implementado, y mantiene, un programa corporativo de seguridad de datos personales razonable y proporcionado."*

Además de lo anterior, la recurrente enuncia y explica lo siguiente en relación con lo mencionado en algunas noticias:

> Zoom ha mitigado el riesgo de ataques sobre credeciales (Credential-Stuffing Attacks), que no son exclusivos de Zoom ni el resultado de problemas de seguridad de Zoom[27]
>
> Zoom ha eliminado la supuesta vulnerabilidad relacionada con los enlaces de chat, que nunca fue explotada, y que habría requerido una violación de sistemas que no son de Zoom.[28]
>
> La recopilación pasada de datos técnicos de dispositivos del SDK de Facebook no era una vulnerabilidad de seguridad[29]
>
> El "LinkedIn Sales Navigator" no implicaba una vulnerabilidad de seguridad[30]
>
> La voluntad de Zoom de llegar al acuerdo propuesto con la FTC no establece que su seguridad sea deficiente[31] Frente a este último punto, la recurrente concluye lo siguiente: "(…) *Debido a que el acuerdo propuesto con la FTC es voluntario, basado en acusaciones no probadas que Zoom no ha admitido que sean ciertas y que la FTC no ha demostrado, el acuerdo con la FTC no puede soportar la imposición de obligaciones a Zoom en virtud de la legislación colombiana. Lo anterior, porque las acusaciones de la FTC se refieren solo a cuestiones pasadas que han sido subsanadas, y porque esas cuestiones no constituían deficiencias en las prácticas de seguridad de Zoom*."

v. Pretensión

- Reiterando los argumentos expuestos en el recurso, la recurrente "*(…) solicita respetuosamente que se revoque o se modifique la decisión contenida en la Resolución*"[32]

---

[26] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 12.
[27] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, págs. 13 y 14.
[28] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, págs. 14 y 15.
[29] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 15.
[30] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 16.
[31] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, págs. 16 y 17.
[32] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, págs. 17 y 18.

QUINTO. Que, mediante Resolución 54172 de 25 de agosto de 2021 la Dirección de Investigación de Protección de Datos Personales resolvió el recurso de reposición confirmando en todas sus partes la Resolución No. 74519 de 23 de noviembre de 2020.

SEXTO. 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. 74519 de 23 de noviembre de 2020, se procede a resolver el recurso interpuesto, de acuerdo con las siguientes,

CONSIDERACIONES DEL DESPACHO

1. **FUNCIONES DEL DESPACHO DEL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES.**

El artículo 16 del Decreto 4886 de 26 de diciembre de 2011[33] establece las funciones del Superintendente Delegado para la Protección de Datos Personales, entre las cuales se destaca la 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.*
>
> *(…)"* (Énfasis añadido)

2. **DE LA NOTIFICACIÓN DE LA RESOLUCIÓN NO. 74519 DEL 23 DE NOVIEMBRE DE 2020**

Señala la recurrente que: "*presenta este recurso de reposición y en subsidio apelación para proteger su derecho a la defensa, así como hizo al presentar la versión anterior de este recurso el 10 de diciembre de 2020*."[34] Lo anterior, añade, sin perjuicio de lo dicho mediante comunicación 20-87350- 17 de 22 de enero de 2021"

Por su parte, en la comunicación mencionada del 22 de enero de 2021, dicha sociedad solicitó lo siguiente:

> "(…) *Modificar o revocar la "Certificación/Informe Notificación" registrado en el portal de la SIC el 20 de enero de 2020 y suscrito por el COORDINADOR GRUPO NOTIFICACIONES Y CERTIFICACIONES en donde se declara que la notificación de la Resolución 74519 de 2020 fue surtida el 13 de enero de 2020, de manera que (i) se surtan las notificaciones respectivas de manera correcta a través de los canales indicados por Zoom, o (ii) se declare que la fecha de notificación que no podrá ser anterior al 21 de enero de 2021, por cuanto solo hasta fecha la SIC habilitó al apoderado de Zoom el acceso al expediente de la referencia*."

Frente al particular, por medio de la resolución 54172 de 25 de agosto de 2021, la Dirección de Investigación de Protección de Datos Personales se refirió a este tema señalando que:

---

[33] 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.
[34] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 3.

"(…) *Sin que el apoderado o la sociedad administrada tuvieran acceso al expediente, la Secretaría General Ad-Hoc de la Superintendencia de Industria y Comercio emitió a los veinte (20) día (s) del mes de enero de dos mil veintiuno (2021) la siguiente certificación de notificación:*

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
RAD: 20-87350- -15 FECHA: 2021-01-20 10:46:14
TRA: 384 PROTECDATOS EVE: 330 INVESTIGACION
ACT: 513 CERTIINFORMENOTIFIC FOLIOS: 1
ORI: 104 G.NOTIFICERTIFI DES: 7100 DIRINVDATOSPERS

LA SECRETARIA GENERAL AD-HOC

CERTIFICA

Que el acto administrativo número 74519 de fecha 23/11/2020 proferido en el expediente 20-87350, fue notificado y/o comunicado en las fechas y a las personas que se indican a continuación:

NOTIFICADO	REPRESENTANTE LEGAL, APODERADO, Y/O AUTORIZADO	FORMA DE NOTIFICACIÓN	NÚMERO DE NOTIFICACIÓN	FECHA DE NOTIFICACIÓN
ZOOM VIDEO COMMUNICATIONS, INC	LYNN HAALAND	Aviso	317	13/01/2021

Se expide a los veinte (20) dia(s) del mes de enero de dos mil veintiuno (2021), con destino a DIRECCIÓN DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES .

ALEJANDRO COY QUINTERO
COORDINADOR GRUPO NOTIFICACIONES Y CERTIFICACIONES

(…)"[35]

Añade la Dirección que: "*Considerando que solo a partir del día veintiuno (21) del mes de enero el apoderado tuvo acceso al expediente (y) [c]on el objetivo de respetar los derechos fundamentales a un debido proceso y el derecho de defensa, esta autoridad accederá a estudiar de fondo el recurso de reposición y en subsidio apelación que presentó Zoom por medio de apoderado*."[36]

Si bien el Despacho comparte la conclusión de la Dirección de estudiar de fondo el recurso presentado, también se debe aclarar que, en todo caso, la recurrente presentó el recurso de reposición y en subsidio de apelación dentro de los diez (10) días siguientes a su notificación, tomando como fecha la certificada por la Secretaría General Ad-Hoc de la Superintendencia de Industria y Comercio (13-01-2012), tal y como lo ordena el artículo 76 de la Ley 1437 de 2011 -Código Administrativo y de lo Contencioso Administrativo CPACA-:

> *"Los recursos de reposición y apelación deberán interponerse por escrito en la diligencia de notificación personal, o* ***dentro de los diez (10) días siguientes a ella****, o a la notificación por aviso, o al vencimiento del término de publicación, según el caso. Los recursos contra los actos presuntos podrán interponerse en cualquier tiempo, salvo en el evento en que se haya acudido ante el juez. (…)" (Destacamos).*

[35] Resolución 54172 de 25 de agosto de 2021, págs 7 y 8.
[36] Resolución 54172 de 25 de agosto de 2021, pág. 9.

En efecto, la Dirección tomó como fecha de presentación del recurso el día 28 de enero de 2021, cuando su fecha de presentación fue el día 27 de enero de 2021 (día 10 para la presentación del recurso), como se muestra a continuación:

"(…)

De:	mjaramillo@gomezpinzon.com		
Enviado el:	2021-01-27 14:59:40		
Para:	contactenos@sic.gov.co <contactenos@sic.gov.co>, csalazar@sic.gov.co <csalazar@sic.gov.co>, habeasdata@sic.gov.co <habeasdata@sic.gov.co>, contactenos@sic.gov.co <contactenos@sic.gov.co>, Mauricio Jaramillo Campuzano <mjaramillo@gomezpinzon.c		
Copia:			
Asunto:	Zoom – Radicado 20-87350 - Recurso de reposición y en subsidio apelación contra la Resolución 74519 de 2020		
Radicación:	20-87350- -00019-0000		
Fecha:	2021-01-28 08:43:00	**Dependencia:**	7100 DIRINVDATOSPERS
Trámite:	384 PROTECDATOS	**Evento:**	330 INVESTIGACION
Actuación:	713 REPOAPELA	**Folios**	48

(Subrayado fuera del texto)

(…)"[37]

De esta manera, el recurso debe ser evaluado de fondo por esta entidad, sobre todo, porque su presentación fue realizada en tiempo, conforme lo ordena la Ley.

Ahora bien, como lo menciona la recurrente y como se evidencia en el sistema de radicación de trámites de esta entidad, el día 10 de diciembre de 2021, esto es, antes de la notificación de la resolución No. 74519 del 23 de noviembre de 2020, la recurrente presentó un primer escrito de recurso de reposición y en subsidio apelación[38], en el que, además de presentar sus argumentos jurídicos, manifestó que: "(…) *para la fecha de la presentación de este documento, Zoom no ha recibido aún una notificación oficial de la Resolución, por lo tanto, la presentación del presente recurso es oportuna."*

De manera posterior, la recurrente radicó un segundo escrito de recurso de reposición y en subsidio apelación en el que dijo, entre otras, lo siguiente: "*(…) Zoom está radicando nuevamente este recurso* ***con ajustes*** *en respuesta a la supuesta notificación por parte de la SIC el 13 de enero de 2021 y basado en la revisión por parte de Zoom de los archivos del expediente, a los cuales no tuvo acceso sino hasta el 21 de enero de 2021. (…)"*[39] (Destacamos).

Dicho lo anterior, entiende el Despacho que el segundo escrito no es un complemento del primero, sino, más bien, un reemplazo del mismo. Así las cosas, considerando que este segundo escrito -27 de enero de 2021- se presentó dentro de los die (10) días siguientes a la notificación de la resolución No. 74519 del 23 de noviembre de 2020, será ese documento, y no el radicado el 10 de diciembre de 2021, el que se tendrá en cuenta a efectos de dar trámite al recurso de apelación que le corresponde fallar al Despacho.

3. ES FALSA LA AFIRMACIÓN DE ZOOM VIDEO COMMUNICATIONS, INC SEGÚN LA CUAL LA ORDEN ADMINISTRATIVA SE FUNDA EN UNA DECISIÓN ESPAÑOLA

Manifiesta la recurrente lo siguiente: *"Los tribunales colombianos han declarado específicamente que los fallos emitidos por autoridades extranjeras en materia de protección*

[37] Comunicación No. 20- 87350- 19 de 27 de enero de 2021.
[38] Comunicación No, 20-873550-10 de 10 diciembre de 2020.
[39] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 1, pie de página No. 1.

de datos no son vinculantes en Colombia -T-277 de 2015- ***La Resolución se basa en la decisión de 2013 de la AEPD-Agencia Española de Protección de Datos****- contra Google (...) sin reconocer la gran disparidad entre el marco de protección de datos español y colombiano, y las cuestiones de hecho que motivaron la Decisión de la AEPD".*[40] (Énfasis añadido)

De la lectura de la resolución 74591 de 23 de noviembre de 2020 se puede constatar que las órdenes emitidas se fundamentaron, entre otras, en las siguientes normas de la República de Colombia: Constitución Política de 1991 (Artículos 4 y 333) Ley Estatutaria 1581 de 2012 (Artículos 2, 3, 4, 17, 18, 19, 21), Decreto 1074 de 2015 (Artículos 2.2.2.25.2.1, 2.2.2.25.6.1, 2.2.2.25.6.2.).

El hecho que se citen casos y decisiones de otras autoridades (*Federal Trade Commission de los Estados Unidos de América -FTC- o la Agencia Española de Protección de Datos -AEPD-*) , no significa que la decisión de esta entidad se fundamente en la regulación de otros países.

Se hizo referencia a la FTC porque, como se indicó en el apartado "IX.**Actuaciones y decisiones de autoridades extranjeras en relación con el Tratamiento de Datos Personales por parte de ZOOM VIDEO COMMUNICATIONS, INC"** de la resolución recurrida, el 9 de noviembre de 2020 la COMISIÓN FEDERAL DE COMERCIO DE LOS ESTADOS UNIDOS DE AMÉRICA ("The Federal Trade Commission") publicó un acuerdo resolutorio (*Agreement Containing Consent Order*) en el que establece que Zoom debe proteger de mejor manera la información personal. [41]

También se citó a la AEPD en la página 5 para destacar que:

> "(…) *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).

Hacer referencia a decisiones de autoridades extranjeras no significa que las decisiones de la Delegatura se tomen con fundamento en la regulación de otros países. Sólo son algunos antecedentes relevantes sobre la recolección de datos personales y el deber de que su Tratamiento se desarrolle en condiciones de seguridad.

Las decisiones de autoridades extranjeras no son fuente de derecho ni vinculantes a esta autoridad, pero nos permiten conocer lo que está sucediendo en otros países respecto de temas que son objeto de investigación por esta Delegatura.

---

[40] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 7.
[41] Resolución 74519 de 23 de noviembre de 2020, pág. 17 y sig.

Las mismas consideraciones son aplicables al caso de las noticias internacionales citadas en la resolución recurrida. Al respecto, manifiesta la investigada lo siguiente:

> " *En la medida en que la Resolución se basa en estos artículos de noticias, ello violaría los principios fundamentales del debido proceso, porque los informes de prensa no son pertinentes ni conducentes conforme el artículo 168 del CGP para establecer en qué medida las supuestas "fallas" realmente existían, y en qué medida dichos supuestos incidentes contradicen el hecho claro de que Zoom ha implementado, y mantiene, un programa corporativo de seguridad de datos personales razonable y proporcionado."*

No es cierto que la decisión de esta autoridad esté basada en "*artículos de noticias*". Se repite, la justificación de las órdenes dadas tiene como única fuente la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias.

Aunque el mundo está dividido territorialmente, no debe olvidarse que, al mismo tiempo, está fusionado tecnológicamente. Por eso, en temas de Tratamiento de datos personales es frecuente que se utilice como referencia casos, normas o documentos extranjeros dentro de los considerandos de las decisiones sin que ello signifique que la decisión se fundamenta en esas referencias. De hecho, la Corte Constitucional cita en la sentencia C-748 de 2011 -*mediante la cual efectuó la revisión integral del texto de la Ley Estatutaria 1581 de 2012*- algunas normas emitidas en Europa, la Organización de las Naciones Unidas, la Organización de Estados Americanos, Los Estados Unidos de América, España, Portugal, Argentina, Uruguay[42]. Eso no quiere decir que las decisiones de la Corte se funden en esas referencias extranjeras.

No es aceptable bajo ninguna medida que se recurra a argumentos contrarios a la verdad para atacar la decisión de esta entidad. Como bien se ha explicado ampliamente en el curso de esta actuación administrativa, Zoom usa cookies para recolectar o tratar Datos personales en el territorio colombiano. Razón suficiente, para que cumpla con lo estipulado en la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias.

En suma, no es cierto que la decisión de esta entidad se funda en una decisión española o en "*artículos de noticias*". Aunque la investigada tiene derecho a la defensa, ello no debe hacerse recurriendo a afirmaciones que carecen de veracidad. Son inaceptables ese tipo de estrategias de defensa jurídica y de argumentos que faltan a la verdad porque no son correctos ni éticos. Adicionalmente, son irrespetuosos con las autoridades de la República de Colombia porque afirman que no estamos obrando dentro del marco legal de nuestro país.

Sobre este punto, la recurrente debe tener presente que la Constitución Política de la República de Colombia establece en el artículo 4 que "(…) *Es deber de los nacionales y de los extranjeros en Colombia acatar la Constitución y las leyes, y* ***respetar*** *y obedecer a las autoridades*" (Destacamos)

4. EL TRATAMIENTO DE DATOS PERSONALES QUE REALIZA ZOOM ESTÁ SUJETO A LA LEGISLACIÓN DE LA REPUBLICA DE COLOMBIA PORQUE RECOLECTA INFORMACIÓN DE CIUDADANOS Y RESIDENTES EN ESTE TERRITORIO.

El artículo 15 de la Constitución Política Colombiana establece el derecho fundamental al debido Tratamiento de Datos personales, de la siguiente manera:

---

[42] Cfr. Numerales 2.1.1.1.2, 2.1.1.1.3., 2.1.1.1.4., 2.25.3.1., 2.1.2.1., 2.18.3.1.,

> *"Todas las personas tienen (…) derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*
>
> ***En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*** *(...)".* (Énfasis añadido).

Asimismo, la Ley Estatuaria 1581 de 2012 se encargó de desarrollar ese derecho constitucional a que se refieren los artículos 15 y 20 de la Constitución Política Nacional, la cual en el literal g) de su artículo 3 define Tratamiento como, "*Cualquier operación o conjunto de operaciones sobre datos* personales*, tales como la recolección, almacenamiento, uso, circulación o supresión".*

De esta manera, se tiene que esta expresión es de carácter y uso técnico, por lo que, es empleada exclusivamente en el lenguaje propio del campo de los Datos personales. Nótese que la definición de Tratamiento tiene varias 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 otro que involucre directa o indirectamente el uso, almacenamiento o circulación de Datos personales. Sobre este punto, la Corte Constitucional señaló en el numeral 2.5.9. de la Sentencia C-748 de 2011 que, "*lo que se pretende con este proyecto es que* ***todas las operaciones o conjunto de operaciones con los datos 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. Puede ser 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 tecnológicamente porque cobija el Tratamiento realizado mediante cualquier medio físico o electrónico.

Dicho lo anterior, y como bien se ha explicado ampliamente en el curso de esta actuación administrativa, Zoom usa *cookies* para recolectar o tratar Datos personales en el territorio colombiano. Razón suficiente para que cumpla con lo estipulado en la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias.

Por tanto, no le haya razón el Despacho a la recurrente al afirmar que : "El *RPDC rige solo para los responsables o encargados que se establecen por sí mismos y llevan a cabo actividades de procesamiento de datos en Colombia, y debido a que Zoom no es un responsable o encargado de este tipo, la SIC no puede ejercer jurisdicción sobre Zoom para regular sus operaciones en los Estados Unidos de América*"[43]

Lo anterior, se reitera, porque el Tratamiento de Datos Personales que realiza Zoom está sujeto a la legislación de la República de Colombia en virtud de la recolección de información de ciudadanos y residentes en este territorio. La Ley Estatutaria 1581 de 2012 es aplicable

[43] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 5.

a Zoom porque recolecta Datos personales por medio de *cookies* que instala en dispositivos móviles y computadores ubicados en Colombia, es decir, realiza un Tratamiento sobre los mismos.

En otras palabras, la Ley 1581 de 2012 fija de manera expresa su ámbito de aplicación "*al tratamiento de datos personales efectuado* ***en territorio colombiano*****".** Entonces, como las *web cookies* se instalan por parte de Zoom en equipos ubicados en Colombia, el Tratamiento de la información recolectada por este medio, se somete al cumplimiento de la Ley 1581 de 2012.

No comparte este Despacho la consideración de la recurrente al mencionar que: "*La afirmación de la SIC de que el uso de cookies permite el ejercicio de la jurisdicción permitiría a la SIC eludir las limitaciones jurisdiccionales del artículo 2 de la Ley 1581 de 2012 con respecto a cualquier empresa cuyo sitio web es accesible dentro de Colombia, esencialmente, todas las empresas del mundo. Este es un argumento insostenible, incompatible con la clara intención del Congreso de que la Ley 1581 de 2012 se aplique únicamente a las actividades de tratamiento de datos que ocurren dentro del territorio colombiano."*[44]

Insostenible e incompatible con la Ley 1581 de 2012 es el argumento de la recurrente que olvida que, entre otras, para recolectar datos en Colombia no es necesario estar domiciliado en este país. Avances y herramientas tecnológicas permiten que empresas u organizaciones recolecten datos en Colombia sin hacer presencia física en nuestro territorio. Estas organizaciones realizan *"presencia tecnológica"* en nuestro territorio mediante el uso de las dichas herramientas o aplicativos que se instalan en los equipos (teléfonos, tabletas, computadores, etc) ubicadas en el territorio colombiano. Esa realidad no puede desconocerse ni ser argumento para eximirse de la aplicación de la regulación colombiano.

No es sensato que quien recolecte y trate datos en el territorio de la República de Colombia sin estar domiciliado o residir en el mismo acuda a argumentos clásicos de territorialidad no solo para para evadir sus responsabilidades legales frentes a las autoridades y los titulares de los datos, sino para desconocer el ámbito de aplicación de la citada ley.

Resulta claro que es la propia legislación colombiana, expedida en el Congreso de la República, la que determina que regulará el Tratamiento efectuado en este país y, además, precisa que la recolección de Datos personales como una operación sobre los mismos, es sin lugar a duda un Tratamiento. Por tanto, no es una afirmación de esta Superintendencia ni una regla "*inventada*" por esta autoridad, es un ejercicio de simple aplicación de la Ley.

En efecto, el Responsable del Tratamiento que emplee las *web cookies* para la recolección de Datos personales en este territorio deberá garantizarle al Titular de la información sus derechos y cumplir los deberes que emanan de la legislación colombiana en materia de Protección de Datos Personales.

Resulta por ello indiscutible que 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 sus Datos.

Se recuerda el principio general de interpretación jurídica, según el cual donde la ley no distingue no le es dado al intérprete hacerlo. De esta manera, si se adelanta recolección de Datos en el territorio colombiano aplica la ley colombiana.

---

[44] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, págs. 6 y 7.

No se comparte, la opinión del apoderado, pues, en todo momento la Superintendencia de Industria y Comercio ha basado sus decisiones en lo establecido por la ley y la regulación colombiana.

5. COOKIES Y RECOLECCIÓN DE DATOS PERSONALES

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, la recurrente 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.

Autoridades de protección de datos de varios países -*Uruguay, España, Irlanda, Reino Unido, Italia y Estados Unidos*- y el Tribunal de Justicia de la Unión Europea (TJUE) se han referido a la definición de *"**cookies**"* y su función. De las mismas se concluye, entre otras:

a) Las *cookies* se instalan en los equipos de las personas (teléfonos celulares, *tablets*, computadoras o cualquier otro dispositivo que almacene información)
b) La finalidad de las *cookies* es recolectar o almacenar Datos personales (nombre de usuario, un identificador único, dirección de correo electrónico, las búsquedas que realiza de cada usuario y sus hábitos de navegación en internet, sitios que una persona visita en la web) y otros tipos de información.
c) Las *cookies* son un mecanismo de rastreo o de seguimiento de las personas. Por ejemplo, permiten realizar trazabilidad detallada de las búsquedas de un usuario en internet o de sus hábitos de navegación
d) La recolección o almacenamiento de información mediante las *cookies* constituye un Tratamiento de Datos personales.

Veamos:

En el caso de la República Oriental del Uruguay, la Unidad Reguladora y de Control de Datos Personales señala lo siguiente en su guía sobre "Cookies y perfiles"[45]:

> "*La cookie es un tipo de archivo que almacena información del usuario y es enviada por un sitio web a través de un navegador.* ***Este archivo se descarga en computadoras, tablets, celulares o cualquier otro dispositivo, con la finalidad de almacenar datos que podrán ser actualizados o recuperados por el responsable de su instalación****.*." (Énfasis añadido)

En el Reino de España, la Agencia Española de Protección de Datos señala lo siguiente en su "Guía sobre el uso de cookies"[46]:

> "*La LSSI resulta aplicable a* ***las cookies entendidas en el sentido señalado al comienzo de esta guía, esto es, como cualquier tipo de dispositivo de almacenamiento y recuperación de datos que se utilice en el equipo terminal de un usuario con la finalidad de almacenar información y recuperar la información ya almacenada****, según establece el artículo 22.2 de la LSSI.*

---

[45] República Oriental del Uruguay, Unidad Reguladora y de Control de Datos Personales. *Cookies y perfiles*. En: https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/documentos/publicaciones/Guia%2Bcookies%2By%2Bperfiles.pdf

[46] Reino de España. Agencia Española de Protección de Datos . Guía sobre el uso de cookies. En: https://www.aepd.es/es/documento/guia-cookies.pdf

> *Las cookies* ***permiten el almacenamiento en el terminal del usuario de cantidades de datos que van de unos pocos kilobytes a varios megabytes****.".* (Énfasis añadido).

Adicionalmente, 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****"*[47]*. (…)*. (Énfasis añadido).

En la República de Irlanda, la Oficina del Comisionado de Protección de Datos publicó en el 2020 su guía sobre "Cookies y otras tecnologías de seguimiento"[48]. En ella, se afirmó que:

> "*Las cookies* ***suelen ser pequeños archivos de texto almacenados en un dispositivo, como una PC****, un dispositivo móvil o cualquier otro dispositivo que pueda almacenar información. Los dispositivos que pueden utilizar cookies también incluyen los llamados dispositivos de "Internet de las cosas" (IoT) que se conectan a Internet.*
>
> *Las cookies cumplen una serie de funciones importantes, que incluyen recordar a un usuario y sus interacciones anteriores con un sitio web. Se pueden usar, por ejemplo, para realizar un seguimiento de los artículos en un carrito de compras en línea o para realizar un seguimiento de la información cuando ingresa detalles en un formulario de solicitud en línea. Las cookies de autenticación también son importantes para identificar a los usuarios cuando inician sesión en servicios bancarios y otros servicios en línea*
> *(…)*
>
> ***La información almacenada en las cookies puede incluir datos personales, como una dirección IP, un nombre de usuario, un identificador único o una dirección de correo electrónico.*** *Pero también puede contener datos no personales como configuraciones de idioma o información sobre el tipo de dispositivo que una persona está usando para navegar por el sitio"*. (Énfasis añadido)."

---

[47] La AEPD concluyó lo siguiente: "*la Agencia Española de Protección de Datos también es competente para decidir sobre el tratamiento llevado a cabo por un responsable no establecido en territorio del Espacio Económico Europeo que ha utilizado en el tratamiento de datos medios situados en territorio español, por lo que debe concluirse, igualmente, que la LOPD es aplicable al presente supuesto y procedente la intervención de la Agencia Española de Protección de Datos, por virtud de lo dispuesto en el artículo 2.1.c) de la LOPD*" (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Resolución R/02892/2013 del 19 de diciembre de 2013. Procedimiento sancionador PS/00345/2013 instruido a las entidades Google Inc. y Google Spain, S.L. Madrid, España).

[48] Cfr. República de Irlanda. Oficina del Comisionado de Protección de Datos (2020) *Guidance note: Cookies and other tracking technologies.* En https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf

En el Reino Unido de Gran Bretaña e Irlanda del Norte, la Oficina de la Comisión de Información publicó su "Guía sobre el uso de cookies y tecnologías similares"[49], en la cual se afirma lo siguiente:

> "**Qué son cookies?**
> *Las cookies son pequeños fragmentos de información, que normalmente constan de letras y números, que los servicios en línea proporcionan cuando los usuarios los visitan. El software en el dispositivo del usuario (por ejemplo, un navegador web) puede almacenar cookies y enviarlas al sitio web la próxima vez que lo visite.*
>
> ***¿Cómo se utilizan las cookies?***
>
> *Las cookies son una tecnología específica que almacena información entre visitas al sitio web. Se utilizan de diversas formas, como, por ejemplo:*
>
> - *recordar lo que hay en una "cesta" al comprar productos en línea;*
> - *ayudar a los usuarios a iniciar sesión en un sitio web;*
> - *analizar el tráfico de un sitio web; o*
> - *seguimiento del comportamiento de navegación de los usuarios.*
>
> *Las cookies pueden ser útiles porque permiten que un sitio web reconozca el dispositivo de un usuario. Se utilizan ampliamente para hacer que los sitios web funcionen o funcionen de manera más eficiente, así como para proporcionar información a los editores del sitio. Sin cookies, o algún otro método similar, los sitios web no tendrían forma de "recordar" nada sobre los visitantes, como cuántos artículos hay en una cesta de compras o si han iniciado sesión."*

La Oficina Garante de la protección de datos personales de la República de Italia publicó este año (2021) sus Directrices para *cookies* y otras herramientas de seguimiento[50], en donde señalan, entre otras, lo siguiente:

> *"**Las cookies son, por regla general, cadenas de texto que los sitios web visitados por el usuario** (los llamados sitios web de 'editores' o 'propios') o diferentes sitios web o servidores web (los llamados 'terceros') **colocan y almacenan en un dispositivo terminal en posesión del usuario**, ya sea directamente, como es el caso de los sitios web de los editores, o indirectamente, como es el caso de los "terceros", es decir, a través de la intermediación de los sitios web de los editores.*
>
> ***Los dispositivos terminales a los que se hace referencia incluyen, por ejemplo, un ordenador, una tableta, un teléfono inteligente o cualquier otro dispositivo capaz de almacenar información**. (…)*
> *(…)*
>
> ***La información codificada en las cookies puede incluir datos personales, como una dirección IP, un nombre de usuario, un identificador único o una dirección de correo electrónico**, pero también puede incluir datos no personales*

---

[49] Cfr. Reino Unido de Gran Bretaña e Irlanda del Norte. Oficina de la Comisión de Información. *Guidance on the use of cookies and similar technologies*. En: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/

[50] Cfr. República de Italia. Oficina Garante de la protección de datos personales (2021) *Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021 [9677876].*
En: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876#english

como la configuración de idioma o información sobre el tipo de dispositivo que está usando una persona para navegar dentro del sitio web.

Por lo tanto, las cookies pueden realizar funciones importantes y diversas, ***incluido el seguimiento de la sesión, el almacenamiento de información de acceso al servidor específica relacionada con la configuración del usuario, facilitar el uso de contenido en línea, etc.*** *Por ejemplo, se pueden utilizar para realizar un seguimiento de los elementos en una cesta de la compra en línea o la información utilizada para completar un formulario informático".* (Énfasis añadido).

La Comisión Federal de Comercio (FTC) de los Estados Unidos de América define e indica los usos de las *cookies* en los siguientes términos:

"*Una cookie es información guardada por su navegador web. Cuando usted visita un sitio web, el sitio puede colocar una cookie en su navegador web para que pueda reconocer su dispositivo en el futuro. Si regresa a ese sitio más adelante, puede leer esa cookie para recordarlo de su última visita y realizar un seguimiento de usted a lo largo del tiempo.*
Usos

- ***Recopilar información sobre las páginas que ve y sus actividades en el sitio***
- ***Permitir que el sitio lo reconozca****, por ejemplo:*
  - *Recordando su ID de usuario*
  - *Ofreciendo un carrito de compras en línea*
  - *Realizar un seguimiento de sus preferencias si vuelve a visitar el sitio web*
- *Personaliza tu experiencia de navegación*
- *Entregar anuncios dirigidos a usted*" [51]. (Énfasis añadido).

La FTC público la guía "Cómo Proteger tu Privacidad en línea"[52], en donde afirma lo siguiente:

"Lo que hay que saber acerca del rastreo en línea

Cookies

Cuando usted visita un sitio web, el sitio podría colocar un archivo llamado una cookie en su navegador o explorador de internet. Los sitios web usan cookies para personalizar su experiencia de navegación en internet. Cuando un sitio web coloca una cookie en su navegador, esa es una ***cookie de origen****. A continuación, se enumeran algunos ejemplos de cómo pueden usar las cookies de origen los sitios web:*

- *Un sitio web de noticias le muestra el estado del tiempo en su localidad y artículos sobre temas de su interés.*
- *Un sitio web recuerda su nombre de usuario o los artículos que dejó en su carro de compras en línea.*

---

[51] United States. Federal Trade Commission. What are cookies? En: https://www.ftc.gov/site-information/privacy-policy/internet-cookies Consultada el 16 de septiembre de 2021.
[52] Estados Unidos de América. Comisión Federal de Comercio. El texto completo de la guía puede consultarse en: https://www.consumidor.ftc.gov/articulos/como-proteger-su-privacidad-en-linea

> *Los sitios web que usted visita suelen permitir que otras compañías también coloquen cookies, por ejemplo, para mostrarle anuncios personalizados o dirigidos de acuerdo a sus intereses. Estas son* ***cookies de terceros****. A continuación, algunos ejemplos de cookies de terceros:*
>
> - *Una compañía de publicidad le coloca una cookie y ve que usted visitó un sitio web sobre carreras a pie. Entonces, cuando usted visita otros sitios web, le muestra un anuncio de calzado deportivo para correr.*
> - *Una compañía analítica usa una cookie para obtener detalles sobre su visita a un sitio web, por ejemplo, cuánto tiempo pasó en ese sitio y qué paginas visitó. Puede usar la información que recolecta para detectar problemas con el sitio y mejorarlo."* (Énfasis fuera de texto).

Adicionalmente, en el año 2012 la Comisión Federal de Comercio (FTC) anunció que Google Inc. acordó pagar una multa civil de US $ 22.5 millones[53]. Lo anterior, con el propósito de resolver los cargos presentados por la autoridad relacionados con el presunto engaño a los usuarios del navegador de Internet Safari. Ya que, se les informó que dicho navegador no instalaría *cookies* de seguimiento ni mostraría anuncios dirigidos a esos usuarios, violando un acuerdo previamente firmado por la empresa y la Comisión.

La FTC señaló:

> "*Google, el desarrollador del motor de búsqueda de internet más popular del mundo, genera miles de millones de dólares en ingresos anuales por la venta de servicios de publicidad en línea, incluida la remisión de anuncios publicitarios dirigidos.* ***Las cookies*** *son pequeños fragmentos de texto de computadora que* ***se utilizan para recopilar información de las computadoras*** *y se pueden usar para mostrar anuncios dirigidos a los consumidores.* ***Al colocar una cookie de seguimiento en la computadora de un usuario, una red publicitaria puede recopilar información sobre las actividades de navegación web del usuario y utilizar esa información para publicar anuncios en línea dirigidos a los intereses del usuario o para otros fines***.
>
> *En su denuncia, la Comisión alegó que durante varios meses del 2011 y 2012,* ***Google instaló una determinada cookie de seguimiento de publicidad en las computadoras de los usuarios*** *que usaban Safari y que visitaban sitios dentro de la red publicitaria "DoubleClick" de Google, aunque Google había dicho previamente a estos usuarios que automáticamente serían removidos de dicho seguimiento, como resultado de la configuración predeterminada del navegador Safari utilizado en Macs, iPhones y iPads*"[54]. (Énfasis fuera de texto).

Finalmente, el Tribunal de Justicia señaló lo siguiente en la sentencia con asunto C-673/17[55] de 1 de octubre de 2019:

---

[53] Cfr. Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser. August 9, 2012. Privacy Settlement is the Largest FTC Penalty Ever for Violation of a Commission Order. En: https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented

[54] Ibídem.

[55] SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 1 de octubre de 2019 en el asunto C-673/17. En: https://curia.europa.eu/juris/document/document.jsf;jsessionid=437F394E00932160C3A97E1093FF4B09?text=&docid=218462&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=6852262

"(…) ***las cookies tienen como finalidad recabar información con fines publicitarios para los productos de las empresas*** *colaboradoras del organizador del juego promocional* (…)"

De la resolución de remisión se desprende que ***las cookies son ficheros que el proveedor de un sitio de Internet coloca en el ordenador de los usuarios de dicho sitio y a los que puede acceder nuevamente, cuando estos vuelven a visitar el sitio, con el fin de facilitar la navegación en Internet o las transacciones o de obtener información sobre el comportamiento de dichos usuarios****.*

(…)

Con carácter preliminar ha de precisarse que, según las indicaciones que figuran en la resolución de remisión, ***las cookies que pueden colocarse en el equipo terminal de los usuarios*** *que participan en el juego con fines promocionales organizado por Planet49 llevan un número que se adjudica a los datos de registro de dicho usuario, quien debe inscribir su nombre y su dirección en el formulario de participación de dicho juego. El órgano jurisdiccional remitente añade que la asociación* ***de ese número y esos datos personaliza los datos almacenados por las cookies cuando el usuario se sirve de Internet, de modo que la recogida de tales datos mediante las cookies constituye un tratamiento de datos personales.*** *Estas indicaciones fueron confirmadas por Planet49, quien subrayó en sus observaciones escritas que el consentimiento correspondiente a la segunda casilla constituye una autorización de recogida y tratamiento de datos personales, y no de información anónima.*

Una vez realizadas estas precisiones, procede señalar que, conforme al artículo 5, apartado 3, de la Directiva 2002/58, los Estados miembros velarán por que únicamente ***se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un usuario*** *cuando dicho usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46".* (Énfasis añadido).

En conclusión, la recurrente mediante mecanismos electrónicos recolecta Datos personales en el territorio de la República de Colombia. Por ende, el Tratamiento de Datos personales que realiza está sujeto a la legislación colombiana. En otras palabras, la Ley Estatutaria 1581 de 2012 le es aplicable porque recolecta Datos personales por medio de *cookies* que instala en dispositivos móviles y computadores ubicados en Colombia, es decir, realiza un Tratamiento sobre los mismos.

6. LA LEY COLOMBIANA APLICA AL TRATAMIENTO DE DATOS EFECTUADO EN EL TERRITORIO COLOMBIANO SIN DISTINGUIR SI EL MISMO SE REALIZA MEDIANTE MECANISMOS FÍSICOS O HERRAMIENTAS TECNOLÓGICAS

La recurrente afirma lo siguiente respecto del ámbito de aplicación de la Ley Estatutaria 1581 de 2012:

"*El alcance limitado de la Ley colombiana es compatible con el artículo 4 de la Constitución colombiana, que deja claro que el derecho colombiano rige para los "nacionales y [...] los extranjeros en Colombia". Zoom no ha establecido una presencia local en Colombia que lo someta al derecho colombiano. Zoom ya ha*

explicado a la SIC que no tiene ninguna filial, sucursal o subsidiaria en Colombia, y que no mantiene servidores para el almacenamiento o procesamiento de datos personales o de información dentro del territorio colombiano, así como tampoco proveedores de servicios de almacenamiento de información y datos"[56] Por lo anterior, reafirma que *"la Ley 1581 de 2012, no permite que la SIC regule las operaciones de tratamiento de datos de Zoom en el extranjero"*[57]

"*El intento de la SIC por ejercer jurisdicción sobre Zoom también es contrario al principio de soberanía nacional. La Corte Constitucional de Colombia - T-462 de 2015-ha reconocido que las naciones solo tienen poder para regular las acciones que ocurren en sus territorios (o cuando el Estado en el que la entidad extranjera tiene su sede ha dado su consentimiento para limitar su propia soberanía, lo cual no es el caso aquí). Zoom tiene su sede en los Estados Unidos de América, y no tiene presencia local en Colombia. Por tanto, sería contrario al principio de soberanía nacional por parte Colombia intentar aplicar sus propias leyes a Zoom."*[58]

(…)

"*Debido a que el RPDC rige solo para los responsables o encargados que se establecen por sí mismos y llevan a cabo actividades de procesamiento de datos en Colombia, y debido a que Zoom no es un responsable o encargado de este tipo, la SIC no puede ejercer jurisdicción sobre Zoom para regular sus operaciones en los Estados Unidos de América"*

No se ajustan a derecho esos argumentos por lo siguiente:

Para establecer el campo de aplicación de la Ley Estatutaria 1581 de 2012 se ha utilizado un principio general de interpretación jurídica según el cual **en donde la ley no distingue, no le es dado al intérprete hacerlo**. Principio que en este caso resulta plenamente aplicable porque la recurrente realiza Tratamiento de Datos en el territorio colombiano mediante el uso de *cookies*. Si la ley colombiana no distingue la forma ni los mecanismos como se realiza el Tratamiento en el territorio colombiano, pues no le corresponde a esta autoridad excluir el uso de *cookies* como una de tales herramientas.

La citada regla de interpretación jurídica ha sido utilizada por la Corte Constitucional y la Corte Suprema de Justicia para adoptar algunas decisiones. A continuación, nos permitimos transcribir lo esencial, no solo para recordar la existencia de ese principio sino para reiterar que esta autoridad no ha hecho nada diferente a aplicar la ley colombiana:

- CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. AUTO INTERLOCUTORIO DE 3 DE MAYO DE 2017 (AP2789-2017. RADICACIÓN N.° 49891. APROBADO ACTA N.º 124) MP. DR. FERNANDO ALBERTO CASTRO CABALLERO[59].: " ***Acorde con el principio interpretativo que reza que donde la ley no distingue no le es dado al interprete hacerlo****, se concluye que si la Ley 1820 no excluyó de manera explícita como destinatarios de sus preceptos a los ex integrantes de las FARC - EP, por ejemplo a causa de anterior desmovilización en los términos de la Ley 975 de 2005 u otra*

[56] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, págs. 4 y 5.
[57] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 5.
[58] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 5.
[59] El texto puede leerse en: En: https://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b2may2017/AP2789-2017.pdf

normatividad, mal podría haberlo hecho como lo hizo en este caso la Sala de Justicia y Paz del Tribunal Superior de Bogotá"

- CORTE CONSTITUCIONAL, SENTENCIA C-317 DEL 3 DE MAYO DE 2012. MP. DRA MARÍA VICTORIA CALLE CORREA[60]. "*Al respecto la Corte considera que **no le asiste razón al demandante** pues si bien la Constitución contiene una atribución expresa de representación gubernamental para la iniciativa legislativa en cabeza de los Ministros, y no una atribución similar para la iniciativa constituyente, **resulta plenamente aplicable al tema, el principio general de interpretación jurídica según el cual donde la norma no distingue, no le corresponde distinguir al intérprete**, no resultando jurídicamente viable deducir, por esta vía, reglas constitucionales implícitas que contrarían el texto mismo del artículo 208 Superior, cuyo mandato general de vocería gubernamental no establece tal diferenciación*." (Énfasis añadido)

- CORTE CONSTITUCIONAL, SENTENCIA C-127 DE 22 DE ABRIL DE 2020. MP. DRA. CRISTINA PARDO SCHLESINGER[61]: "*Por lo anterior, **en desarrollo del principio general de interpretación jurídica según el cual donde la norma no distingue, no le corresponde distinguir al intérprete**, no resulta viable deducir la existencia de la regla de exclusión implícita a que aluden los demandantes*." (Énfasis añadido).

Se enfatiza que en esta actuación administrativa no existe ningún "*intento de la SIC por ejercer jurisdicción sobre Zoom*" porque esta entidad no actúa bajo un libre albedrío, sino que simplemente aplica la Ley colombiana de Protección de Datos y, en particular, lo que ordena el artículo 2 de la citada ley, a saber: ***" 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*" (Énfasis añadido).

Como se mencionó, tanto para la Constitución de la República de Colombia como para la precitada ley es importante la **recolección** y el **Tratamiento** de Datos sin que sea relevante si la misma se realiza mediante mecanismos manuales, automatizados o si se recurre al uso de tecnologías *(cookies)* conocidas o por conocer para dicho efecto.

Se recalca que, el literal g) del artículo 3 de la Ley Estatutaria 1581 de 2012 define Tratamiento como, "***Cualquier operación o conjunto de operaciones sobre datos* personales*, tales como la recolección**, almacenamiento, uso, circulación o supresión".* (Énfasis añadido). Esa definición legal es neutral tecnológicamente porque cobija el Tratamiento realizado mediante cualquier medio físico o electrónico como, entre otras, las *"cookies".* La recurrente realiza Tratamiento de Datos personales en territorio colombiano porque usa *cookies* para recolectar Datos personales en el territorio de la República de Colombia. Razón suficiente, para que de conformidad con lo establecido en el artículo 2 de la Ley Estatutaria 1581 de 2012 cumpla con lo estipulado en dicha ley y sus normas reglamentarias.

En virtud de lo anterior, no asiste razón a la recurrente en cuanto a que no le es aplicable la Ley Estatutaria 1581 de 2012.

---

[60] El texto completo de la sentencia puede consultarse en: https://www.corteconstitucional.gov.co/relatoria/2012/C-317-12.htm

[61] La sentencia puede consultarse en: https://www.corteconstitucional.gov.co/Relatoria/2020/C-127-20.htm

7. DE LOS CONCEPTOS DE LAS AUTORIDADES ADMINISTRATIVAS Y SU CARÁCTER NO VINCULANTE

La recurrente cita de manera reiterada los siguientes conceptos No. 14-218349-3 (2014)-[62] y 16-172268-1 (2016)-"[63], así:

> "*La propia SIC, en respuesta a un derecho de petición confirmó que el RPDC no le permitía regular el tratamiento de datos por parte de Facebook a través de Internet, porque "dicha compañía en la actualidad no tiene domicilio en Colombia*" -Consulta Pública No. 14-218349-3 (2014)-[64]

> "*La SIC ha reconocido que la situación jurídica de las cookies conforme a la legislación colombiana no es clara, y únicamente afirma que puede "eventualmente" determinarse que las cookies puedan, en determinados contextos fácticos, tratar datos personales - Respuesta Derecho de Petición radicado No. 16-172268-1 (2016)-"*[65]

Frente al particular, como es sabido, **los conceptos jurídicos no son de obligatorio cumplimiento**, lo anterior de acuerdo con el artículo 28 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo:

> *"Alcance de los conceptos. Salvo disposición legal en contrario**, los conceptos emitidos por las autoridades como respuestas a peticiones realizadas en ejercicio del derecho a formular consultas no serán de obligatorio cumplimiento o ejecución**".* (Énfasis añadido).

Así las cosas, considerando que en el transcurso de esta actuación administrativa se han explicado los motivos de hecho y de derecho que motivan la decisión adoptada, lo que se mencione en dichos conceptos en nada afecta la rigurosidad y legalidad de las órdenes dadas a la recurrente.

Ahora bien, a pesar de lo anterior y solo en gracia de discusión, vale la pena mencionar el Concepto 14-218349 de 3 de marzo de 2016 en el cual en relación con el ámbito de aplicación de la Ley Estatutaria 1581 de 2012 se dijo:

> *"(...) Sin duda alguna, el precepto jurídico citado extiende el ámbito de aplicación de la ley estatutaria de protección de datos personales a un sinnúmero de escenarios de tratamiento de información personal en Colombia, verbigracia, de manera ilustrativa, el tratamiento de datos personales efectuado por proveedores de servicios de redes sociales establecidos fuera del país, a través de un "medio"*[20] *situado en territorio colombiano. Con el fin de otorgar mayor claridad en el tema, esta Superintendencia se permite referir lo expuesto en el Informe de Trabajo No. 56, del grupo de trabajo del artículo 29 de la Directiva 95/46/CE, relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE, el cual indicó que*

> *"(...) los PC, los terminales y los servidores, que se pueden utilizar para casi todos los tipos de operaciones de tratamiento de datos, son ejemplo de medios"*[21]

---

[62] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 4.
[63] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 6.
[64] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 4.
[65] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 6.

Interpretación conforme con el entendimiento que ha tenido la Corte Constitucional sobre el asunto en Colombia, dado que en Sentencia C-748 de 2011, manifiesta que dentro de los medios informáticos de divulgación o comunicación masiva, se encuentran las redes sociales y la internet, otorgándole gran importancia a la determinación de los medios de tratamiento utilizados, toda vez que es uno de los parámetros que contribuye a la identificación del responsable del tratamiento de datos personales[22].

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

(...)

Al tenor de lo anterior, se colige que el deseo del legislador estatutario y de la Corte Constitucional desde el punto de vista del ámbito de aplicación de la ley estatutaria de protección de datos personales, es evitar que una persona quede desprotegida durante el tratamiento de sus datos por la única razón de que el responsable y/o encargado del tratamiento no se encuentre establecido en el territorio colombiano. (...)"

8. DE LA FACULTAD LEGAL DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO PARA EMITIR ÓRDENES

Como es sabido, el artículo 19 de la Ley Estatutaria 1581 de 2012, le otorgó competencia a esta entidad, a través de la Delegatura para la Protección de Datos Personales, para ejercer: "*(…) la vigilancia necesaria para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.*"

Asimismo, el artículo 21 determina las funciones que debe cumplir la Superintendencia de Industria y Comercio, en virtud de la competencia conferida por el artículo 19 mencionado:

"***ARTÍCULO 21. FUNCIONES.*** *La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:*

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, existen expresas y suficientes facultades legales para que esta autoridad pueda impartir órdenes o instrucciones con miras a proteger el derecho al debido tratamiento de los datos personales.

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."*

Así, la ley colombiana faculta a la Superintendencia de Industria y Comercio no solo para emitir órdenes o instrucciones sino para exigir el debido Tratamiento de los Datos personales. Por eso, emitir una orden es un acto respetuoso del marco legal.

Finalmente, y no menos importante, de la lectura del artículo 23 de la Ley Estatutaria 1581 de 2012 se puede constatar que **las órdenes no son sanciones**:

> *"**ARTÍCULO 23. SANCIONES.** La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:*
>
> *"a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;*
>
> *b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;*
>
> *c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;*
>
> *d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;"*

Dado lo anterior, para la emisión de una orden no es necesario observar las pautas del procedimiento administrativo sancionatorio a que se refiere el artículo 47 y siguientes de la ley 1437 de 2011.

En suma, las órdenes no son sanciones sino son medidas necesarias para, entre otras, hacer efectivo el derecho al debido tratamiento de datos personales o para que los Responsables del Tratamiento y Encargados del Tratamiento cumplan correctamente los previsto en regulación con miras a garantizar el debido Tratamiento de los datos personales y el respeto de los derechos de los Titulares de los datos. Por ende, son consistentes con la regulación de Tratamiento de datos personales las órdenes emitidas mediante la resolución recurrida.

9. DEL DEBIDO PROCESO EN LA ACTUACIÓN ADMINISTRATIVA

Respecto del derecho de defensa, se deben reiterar varias cosas:

Dice la recurrente que "*Zoom no tuvo la oportunidad adecuada de contradecir las pruebas invocadas por la SIC en la Resolución porque* el *Requerimiento no citó el artículo de "Bleeping Computer", el artículo de "Hacker News", el artículo de "Vice" o el artículo de "New York Times", en los que ahora se basa la Resolución."* Además, añade que: "*La SIC tampoco le dio a Zoom la oportunidad de explicar su uso de cookies antes de utilizar ese argumento como fundamento para su jurisdicción (…)* "*(L)a Resolución se basa en gran medida en el anuncio de la FTC de la propuesta de acuerdo voluntario con Zoom, que se anunció a principios de noviembre, y sobre el cual la SIC no hizo ninguna pregunta a Zoom. (…)*

Las anteriores afirmaciones no son ciertas dado que la resolución 74519 de 23 de noviembre de 2020 no se basó, ni está fundamentada en dichos artículos. Como ya se explicó, la cita tanto de decisiones de autoridades extranjeras, como de algunos artículos periodísticos tuvieron como fin servir de antecedentes que se consideraron útiles y un buen ejercicio a la hora de conocer lo que ocurre en el extranjero. Se repite, las órdenes dadas a Zoom tuvieron como único fundamento jurídico la Ley de Protección de Datos de la República de Colombia.

Ahora bien, las órdenes dadas a la investigada están relacionadas con la adopción de medidas de seguridad, tema que fue justamente el que se abordó en el requerimiento inicial realizado a la recurrente. Entonces, si el oficio inicial fue sobre seguridad en el Tratamiento de datos, es totalmente congruente que la orden sea la de implementar medidas de seguridad, veamos:

En requerimiento realizado el catorce (14) de abril de 2020 a la investigada se le solicitaba informar a esta autoridad lo siguiente:

> "*1. ¿Existen ciudadanos Colombianos afectados por incidentes de seguridad presentados en la plataforma Zoom, tales como robo de credenciales de usuarios y la información intercambiada en las reuniones, transferencias de información a Facebook, robo de credenciales de Microsoft, acceso a los perfiles de LinkedIn, entre otros presentados durante el año 2020?*
> *2. ¿Cuál es la cantidad de ciudadanos o personas residentes en la República de Colombia que se han visto afectados por incidentes de seguridad presentados en la plataforma Zoom durante el año 2020?*
> *3. ¿Se han presentado reclamos de los ciudadanos o residentes en el Estado Colombiano afectados, si es así cual fue la gestión realizada en estos casos?*
> *4. ¿Cuáles fueron las medidas para solucionar cada incidente de seguridad y cuáles fueron las medidas para evitar que se presentara nuevamente?*
> *5. Para el caso de las reuniones realizadas en ZOOM, las grabaciones guardadas en la nube, ¿los servidores donde se encuentran geográficamente?*
> *6. ¿Quien tiene acceso a las grabaciones de la nube?*
> *7. ¿Cuándo se programa una reunión la información recolectada en el registro previo, donde*
> *guarda los datos recolectados, quien es Responsable de la información?*
> *8. Informe qué datos recolecta en cada plataforma en que funciona la aplicación además de:*
> *1. Nombre de usuario.*
> *2. Dirección física.*
> *3. Dirección de correo electrónico.*
> *4. Número de teléfono.*
> *5. Información de trabajo.*

6. Información de perfil de Facebook.
7. Especificaciones de computadora o teléfono.
8. Dirección IP.
9. Ubicación.
10. Zona horaria de los usuarios.
9. ¿Con qué empresas, plataformas, entidades las aplicaciones de ZOOM realizan intercambio o envió de datos del Titular? Y ¿por qué causa?
10. ¿Donde se encuentran y como se obtienen las autorizaciones de los Titulares para el Tratamiento de los datos tratados por los terceros?
11. ¿Cuál es la información que se comparte y/o trasmite en cada caso?
12. ¿Que Tratamiento de información o datos es aplicado por cada tercero?
13. ¿Que políticas de seguridad y privacidad aplicada uno de los terceros a los datos trasmitidos?
14. Adjunten las políticas de gestión de vulnerabilidades de las diferentes versiones de ZOOM
15. Si las recomendaciones de seguridad para el uso de la plataforma de ZOOM no son atendidas
y configuradas por los administradores de las reuniones, qué controles se han implementado para evitar las vulneraciones"[66]

En dicho requerimiento, además, se le informó a la recurrente lo siguiente:

"(...) la iniciación de una actuación administrativa a ZOOM VIDEO COMMUNICATIONS, INC la cual se regirá por lo dispuesto en el Capítulo I del Título III de la Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo).

La presente tiene como propósito establecer si ZOOM VIDEO COMMUNICATIONS, INC cumple con la regulación colombiana relativa a ***los principios de seguridad, acceso y circulación restringida (artículos 4 literales f) y g) y 17 literales d) i) y n) de la Ley 1581 de 2012 en concordancia con el artículo 19 del Decreto 1377 de 2013 incorporado en el Decreto 1074 de 2015****). Y,* ***si la misma ha implementado el principio de responsabilidad demostrada en esa materia (artículos 26 y 27 del Decreto 1377 de 2013 incorporado en el Decreto 1074 de 2015).***"[67]

El 13 de mayo de 2020 Zoom respondió dicho requerimiento, esto es, pasado casi un mes, en el que, por supuesto, tuvo la oportunidad de preparar la información y enviar a esta Superintendencia todo lo que considerara oportuno.

Por su parte, las órdenes dadas a la recurrente en la resolución 74519 de 23 de noviembre de 2020 están relacionadas de manera congruente con la seguridad de los datos personales Tratados en el territorio colombiano, que fue sobre lo que versó el requerimiento, veamos:

ARTÍCULO PRIMERO. *ORDENAR a la sociedad ZOOM VIDEO COMMUNICATIONS, INC en adelante Zoom, 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:*

---

[66] Radicado No. 20- 87350-01 de 14 de abril de 2020.
[67] Radicado No. 20- 87350-01 de 14 de abril de 2020.

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 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 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 Zoom;
c) La naturaleza y el ámbito de las actividades de Zoom;
d) La cantidad de Titulares;
e) La naturaleza de los Datos personales;
f) El tipo de Tratamiento de los Datos personales;
g) El alcance, contexto y fines del Tratamiento;
h) Las actualizaciones o cualquier tipo de modificación de la plataforma de Zoom, sus productos y cualquier otra forma en que Zoom utilice, recopile, comparta o trate los datos recolectados;
i) El acceso a los Datos personales por parte de los empleados, contratistas y en general los colaboradores de Zoom;
j) El uso de los Datos personales de los usuarios por terceros, entre ellos, aliados
comerciales, empresas asociadas y desarrolladores de aplicaciones, si aplica;
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 personales; y
m) Los riesgos para los derechos y libertades de los Titulares.

3) Desarrollar, implementar y mantener un programa de gestión y manejo de incidentes de seguridad en Datos personales, que contemple procedimiento para información sin dilación indebida a esta Superintendencia de Industria y Comercio y a los Titulares de los mismos cuando se presenten incidentes que afecten la confidencialidad, integridad y disponibilidad de los Datos 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 personales y su política de Tratamiento de Datos personales (o privacidad) de Zoom.

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)Zoom 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, certificar a esta entidad que cuenta con las medidas técnicas, humanas, administrativas, contractuales y de cualquier otra naturaleza que sean necesarias para otorgar seguridad a los Datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."*

Adicional a todo lo anterior, Zoom ha contado con las oportunidades procesales dispuestas por la Ley para presentar los recursos que considere necesarios a la resolución 74519 de 23 de noviembre de 2020, eso es tan así que precisamente este acto administrativo tiene como fundamento el ejercicio del derecho de defensa de la investigada.

De otro lado, también argumenta Zoom que la resolución no se basa en pruebas adecuadas ni en un análisis jurídico. Indica la recurrente que "*La SIC ha ignorado (o no ha ofrecido a Zoom una oportunidad justa para probar) que la seguridad de Zoom sería adecuada conforme al RPDC, y la SIC no ha podido establecer ningún hecho que respalde su conclusión de que la seguridad de Zoom es inadecuada*."[68] "*La SIC no tuvo en cuenta las medidas de seguridad actuales de Zoom ni probó que se hayan violado, no presentó ninguna prueba sobre las prácticas de seguridad de Zoom (invocando solo un puñado de artículos de noticias, más una queja presentada por la FTC), y no presentó ningún sustento jurídico que respaldara su imposición de cargas regulatorias onerosas a Zoom*"[69]

Además, añade que: *"(L)a mera mención de que "aún subsisten algunas falencias" no constituye un análisis jurídico suficiente para justificar las onerosas obligaciones de cumplimiento establecidas en la Resolución, en particular porque todas las acusaciones de los artículos de noticias y la queja de la FTC se refieren a cuestiones que, para empezar, no eran vulnerabilidades de seguridad, o bien que ya han sido atendidas por Zoom.* "(*E)l "Análisis Técnico" que fue realizado por la SIC no provee ni sustenta la afirmación por parte de la SIC en la Resolución de que "aún subsisten algunas falencias". Al contrario, el Análisis Técnico no identifica ninguna vulnerabilidad de seguridad actual, y en cambio, confirma que Zoom ha resulto los posibles problemas que fueron citados en la Resolución*" [70]

Este Despacho no está de acuerdo con esas afirmaciones por lo siguientes motivos:

No es cierto que esta autoridad "*no ha ofrecido a Zoom una oportunidad justa para probar que la seguridad de Zoom sería adecuada conforme al RPDC",* como se explicó ampliamente, claro que Zoom tuvo la oportunidad de probar a esta entidad qué medidas de ha adoptado. Esto es tan evidente que el requerimiento realizado tuvo como objeto principal indagar sobre la seguridad en el Tratamiento de Datos Personales realizado por Zoom. No es responsabilidad de esta entidad, sino únicamente de la recurrente, el no haber contestado ese requerimiento con la suficiencia para demostrar su debido cumplimiento de la Ley.

También es falso que no se hayan probado las vulneraciones a la seguridad en el Tratamiento de Datos de la Plataforma. A continuación, se extraen los apartes de la resolución recurrida que evidencian dichas falencias:

---

[68] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 9.
[69] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 8.
[70] Comunicación No. 20- 87350- 19 de 27 de enero de 2021, pág. 9.

(i) "*En la parte inferior de la pantalla se encuentra el siguiente mensaje "Zoom está protegido por reCAPTCHA y la Política de privacidad política de privacidad y las Condiciones de servicio aplicables", sin embargo, no se ejecuta o muestra algún método de reCAPTCHA. Por tanto, esta autoridad encuentra como engañosa y falsa dicha afirmación.*

Imagen 3: *Inicio de Sesión Zoom - https://zoom.us/signin, obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

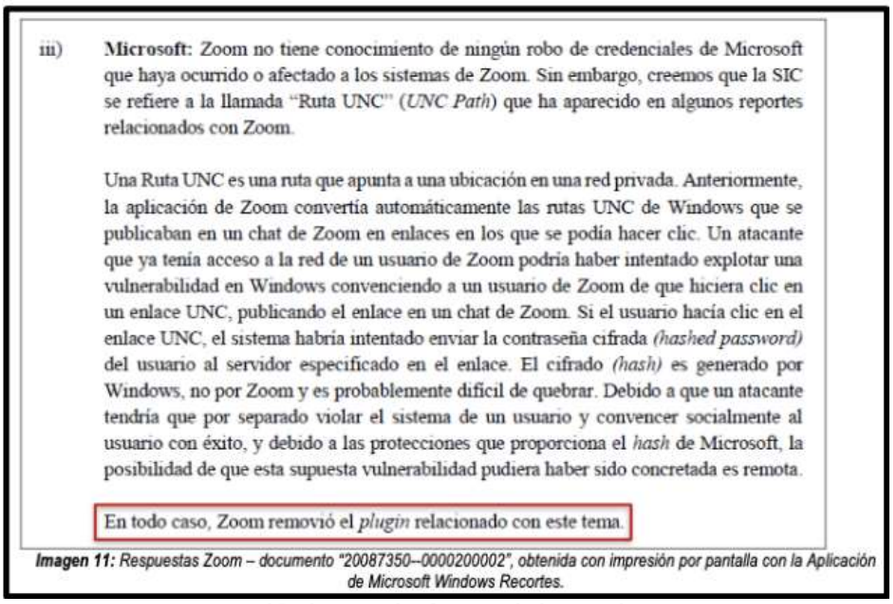
(Subrayado fuera del texto)

(…)"[71]

(ii) "*El robo de credenciales de Windows es una vulnerabilidad en la que los atacantes podían realizar desde el chat de la aplicación de escritorio de la aplicación Zoom para Windows. El robo de las credenciales de inicio de sesión, según el artículo publicado por el portal web "The Hacker News" titulado: "**El nuevo Zoom hack permite a los pitaras informáticos comprometer Windows y su contraseña de inicio de sesión**" se resalta que "todo lo que un atacante debe hacer es enviar una URL creada (es decir, \\ xxxx \ abc_file) a una víctima a través de una interfaz de chat."[17] En el mencionado artículo se adjuntan las pruebas realizadas por "Mohamed Baset" en las que se puede ver cómo funciona el ataque. (…)*

En relación con lo anterior, en su respuesta la compañía afirma lo siguiente:

[71] Resolución 74519 de 23 de noviembre de 2020. Pág. 14.



iii) **Microsoft:** Zoom no tiene conocimiento de ningún robo de credenciales de Microsoft que haya ocurrido o afectado a los sistemas de Zoom. Sin embargo, creemos que la SIC se refiere a la llamada "Ruta UNC" (*UNC Path*) que ha aparecido en algunos reportes relacionados con Zoom.

Una Ruta UNC es una ruta que apunta a una ubicación en una red privada. Anteriormente, la aplicación de Zoom convertía automáticamente las rutas UNC de Windows que se publicaban en un chat de Zoom en enlaces en los que se podía hacer clic. Un atacante que ya tenía acceso a la red de un usuario de Zoom podría haber intentado explotar una vulnerabilidad en Windows convenciendo a un usuario de Zoom de que hiciera clic en un enlace UNC, publicando el enlace en un chat de Zoom. Si el usuario hacía clic en el enlace UNC, el sistema habría intentado enviar la contraseña cifrada *(hashed password)* del usuario al servidor especificado en el enlace. El cifrado *(hash)* es generado por Windows, no por Zoom y es probablemente difícil de quebrar. Debido a que un atacante tendría que por separado violar el sistema de un usuario y convencer socialmente al usuario con éxito, y debido a las protecciones que proporciona el *hash* de Microsoft, la posibilidad de que esta supuesta vulnerabilidad pudiera haber sido concretada es remota.

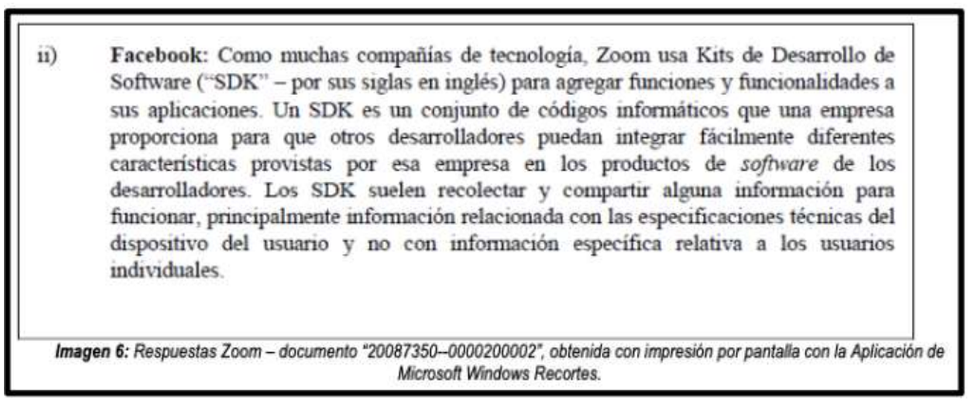
En todo caso, Zoom removió el *plugin* relacionado con este tema.

Imagen 11: *Respuestas Zoom – documento "20087350--0000200002", obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

(Subrayado fuera del texto)

(…)[72]

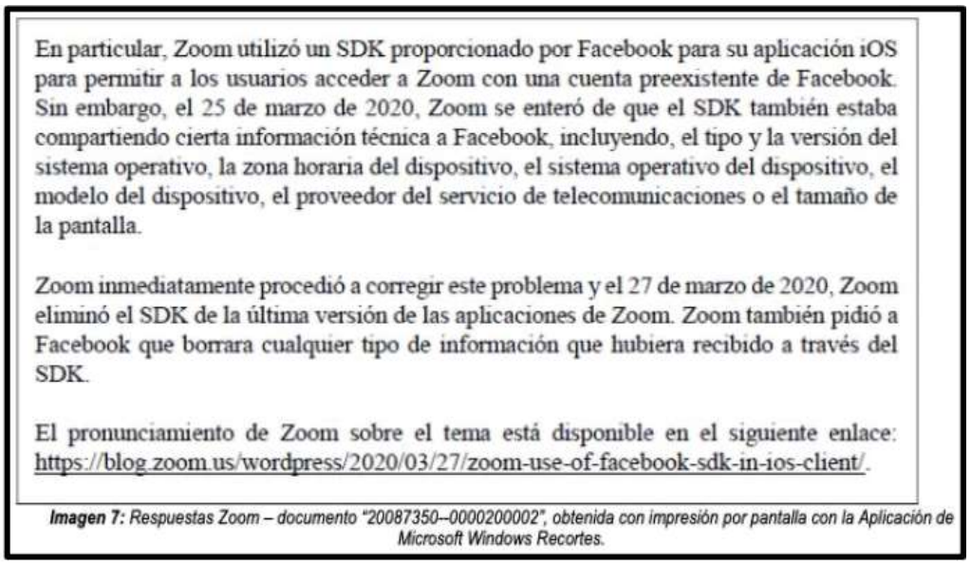
(iii) "De acuerdo con la información entregada por Zoom a esta entidad, en el documento "20087350-- 0000200002", en la página 4 numeral ii), la compañía afirma que "*el 25 de marzo de 2020,* ***Zoom se enteró de que el SDK también estaba compartiendo cierta información técnica a Facebook, incluyendo, el tipo y la versión del sistema operativo, la zona horaria del dispositivo, el sistema operativo del dispositivo, el modelo del dispositivo, el proveedor del servicio de telecomunicaciones o el tamaño de la pantalla.*** *Zoom inmediatamente procedió a corregir este problema y el 27 de marzo de 2020, Zoom eliminó el SDK de la última versión de las aplicaciones de Zoom. Zoom también pidió a Facebook que borrara cualquier tipo de información que hubiera recibido a través del SDK*." (destacamos), como se puede ver a continuación:



ii) **Facebook:** Como muchas compañías de tecnología, Zoom usa Kits de Desarrollo de Software ("SDK" – por sus siglas en inglés) para agregar funciones y funcionalidades a sus aplicaciones. Un SDK es un conjunto de códigos informáticos que una empresa proporciona para que otros desarrolladores puedan integrar fácilmente diferentes características provistas por esa empresa en los productos de *software* de los desarrolladores. Los SDK suelen recolectar y compartir alguna información para funcionar, principalmente información relacionada con las especificaciones técnicas del dispositivo del usuario y no con información específica relativa a los usuarios individuales.

Imagen 6: *Respuestas Zoom – documento "20087350--0000200002", obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

[72] Resolución 74519 de 23 de noviembre de 2020. Pág. 15.



En particular, Zoom utilizó un SDK proporcionado por Facebook para su aplicación iOS para permitir a los usuarios acceder a Zoom con una cuenta preexistente de Facebook. Sin embargo, el 25 de marzo de 2020, Zoom se enteró de que el SDK también estaba compartiendo cierta información técnica a Facebook, incluyendo, el tipo y la versión del sistema operativo, la zona horaria del dispositivo, el sistema operativo del dispositivo, el modelo del dispositivo, el proveedor del servicio de telecomunicaciones o el tamaño de la pantalla.

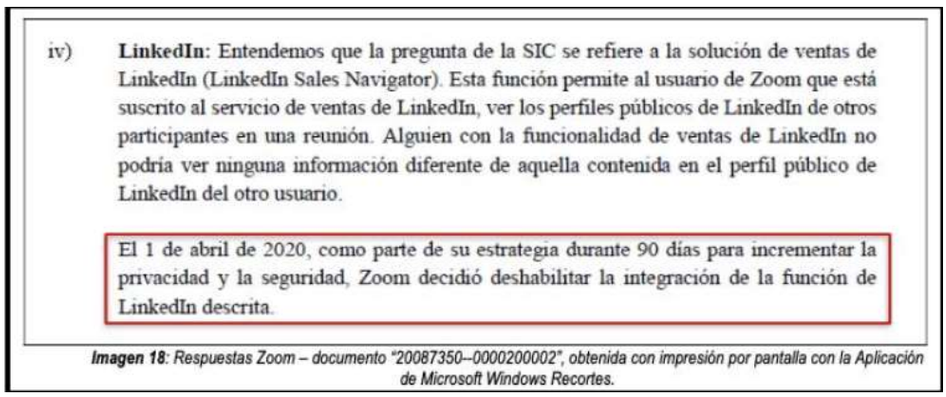
Zoom inmediatamente procedió a corregir este problema y el 27 de marzo de 2020, Zoom eliminó el SDK de la última versión de las aplicaciones de Zoom. Zoom también pidió a Facebook que borrara cualquier tipo de información que hubiera recibido a través del SDK.

El pronunciamiento de Zoom sobre el tema está disponible en el siguiente enlace: https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/.

Imagen 7: *Respuestas Zoom – documento "20087350--0000200002", obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

(…)"[73]

(iv) "*El acceso a los perfiles de la red social LinkedIn a través de la aplicación Zoom se realizaba gracias a la solución de ventas de esta red social, denominada "LinkedIn Sales Navigator". Lo anterior, lo expresa Zoom en el documento "20087350--0000200002" en la página 5, numeral iv), en los siguientes términos:*



iv) **LinkedIn**: Entendemos que la pregunta de la SIC se refiere a la solución de ventas de LinkedIn (LinkedIn Sales Navigator). Esta función permite al usuario de Zoom que está suscrito al servicio de ventas de LinkedIn, ver los perfiles públicos de LinkedIn de otros participantes en una reunión. Alguien con la funcionalidad de ventas de LinkedIn no podría ver ninguna información diferente de aquella contenida en el perfil público de LinkedIn del otro usuario.

El 1 de abril de 2020, como parte de su estrategia durante 90 días para incrementar la privacidad y la seguridad, Zoom decidió deshabilitar la integración de la función de LinkedIn descrita.

Imagen 18*: Respuestas Zoom – documento "20087350--0000200002", obtenida con impresión por pantalla con la Aplicación de Microsoft Windows Recortes.*

(Subrayado fuera del texto)

(…)"[74]

Finalmente, añade la recurrente que: "*Ni la Resolución ni el Análisis Técnico contienen constataciones de que los datos personales de cualquier residente colombiano hayan estado alguna vez sujetos a adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".*

Acá debe recordarse el carácter de orden de la decisión impartida por medio de la resolución recurrida, cuyo objetivo es PREVENTIVO. Esto quiere decir que basta el detectar vulnerabilidades en la plataforma de Zoom para impartir la orden.

Las órdenes no son sanciones sino son medidas necesarias para, entre otras, hacer efectivo el derecho a la Protección de Datos con miras a garantizar el debido tratamiento de los datos personales y el respeto de los derechos de las personas Titulares de la información.

---

[73] Resolución 74519 de 23 de noviembre de 2020. Pág. 16.
[74] Resolución 74519 de 23 de noviembre de 2020. Pág. 17.

En suma, los argumentos que presenta el apoderado no son conducentes ni pertinentes para desvirtuar lo dicho en la decisión contenida en la Resolución No. 74519 de 23 noviembre de 2020.

10. SIN SEGURIDAD NO EXISTE DEBIDO TRATAMIENTO DE DATOS PERSONALES

Las órdenes dadas a Zoom por medio de la Resolución 74519 de 23 de noviembre de 2020 tienen, esencialmente, el objetivo de que se garantice por parte de la investigada, en la práctica, el principio de seguridad en el Tratamiento de los Datos Personales, así como la adecuación de sus operaciones en la República de Colombia a las disposiciones de la Ley Estatutaria 1581 de 2012.

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*"[75] y a "*conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"* [76]; sino que, se reitera, les exige "*(…) ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012"*[77]*.*

De esta manera, cualquier empresa debe ser muy diligente para garantizar el debido tratamiento de los datos personales y el respeto de los derechos de sus Titulares. Por eso, la recurrente no debería ahorrar esfuerzos para mejorar los niveles de seguridad que exige la regulación para todos los usuarios de sus servicios.

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

Se reitera que, la orden impartida es de carácter **PREVENTIVO,** para evitar que se afecte la seguridad de los Datos de los colombianos. 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 la recurrente para garantizar en la práctica, la seguridad de los Datos personales y de los ciudadanos usuarios de sus servicios.

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

Aunque las razones anteriores son suficientes para confirmar la Resolución No. 74519 de 23 noviembre de 2020, esta Delegatura considera pertinente destacar lo siguiente respecto de:

i. Responsabilidad Demostrada (*Accountability*) y "*Compliance*" en el Tratamiento de Datos Personales, y
ii. Responsabilidad Personal de los Administradores

[75] Cfr. Literal g) del artículo 4 de la Ley Estatutaria 1581 de 2012
[76] Cfr. Literal d) del artículo 17 de la Ley Estatutaria 1581 de 2012
[77] Cfr. Artículo 26 del decreto 1377 de 2013 (incorporado en el Decreto 1074 de 2015)

11. RESPONSABILIDAD DEMOSTRADA *(ACCOUNTABILITY)* Y *"COMPLIANCE"* EN EL TRATAMIENTO DE DATOS PERSONALES.

La regulación colombiana le impone al Responsable o al Encargado del Tratamiento, la responsabilidad de garantizar la eficacia de los derechos del Titular del Dato, la cual no puede ser simbólica, ni limitarse únicamente a la formalidad. Por el contrario, debe ser real y demostrable. Al respecto, nuestra jurisprudencia ha determinado que "*existe un deber constitucional de administrar correctamente y de proteger los archivos y bases* [sic] *de datos* [sic] *que contengan información personal o socialmente relevante*"[78].

Adicionalmente, es importante resaltar que los Responsables o Encargados del Tratamiento de los Datos, no se convierten en dueños de los mismos como consecuencia del almacenamiento en sus bases o archivos. En efecto, al ejercer únicamente la mera tenencia de la información, solo tienen a su cargo el deber de administrarla de manera correcta, apropiada y acertada. Por consiguiente, si los sujetos mencionados actúan con negligencia o dolo, la consecuencia directa sería la afectación de los derechos humanos y fundamentales de los Titulares de los Datos.

En virtud de lo anterior, el Capítulo III del Decreto 1377 de 27 de junio de 2013 -incorporado en el Decreto 1074 de 2015- reglamenta algunos aspectos relacionados con el Principio de Responsabilidad Demostrada.

El artículo 26[79] *-Demostración-* establece que, "*los responsables* [sic] *del tratamiento* [sic] *de datos* [sic] *personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012*". Así, resulta imposible ignorar la forma en que el Responsable o Encargado del Tratamiento debe probar poner en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación. Es decir, se reivindica que un administrador no puede utilizar cualquier tipo de políticas o herramientas para dicho efecto, sino solo aquellas que tengan como propósito lograr que los postulados legales sean realidades verificables, y no solo se limiten a creaciones teóricas e intelectuales.

El artículo 27 *-Políticas Internas Efectivas-*, exige que los Responsables del Tratamiento de Datos implementen medidas efectivas y apropiadas que garanticen, entre otras: "(*…) 3. La*

---

[78] Cfr. Corte Constitucional, sentencia T-227 de 2003.

[79] El texto completo del artículo 26 del Decreto 1377 de 2013 ordena: *"Demostración. Los responsables* [sic] *del tratamiento* [sic] *de datos* [sic] *personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto, en una manera que sea proporcional a lo siguiente:*

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

2. La naturaleza de los datos [sic] *personales objeto del tratamiento* [sic]*.*

3. El tipo de Tratamiento.

4. Los riesgos potenciales que el referido tratamiento [sic] *podrían causar sobre los derechos de los titulares* [sic]*.*

En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos [sic] *personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos* [sic] *personales en cada caso.*

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

adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares [sic]*, con respecto a cualquier aspecto del tratamiento* [sic].”[80]

Ahora, respecto de la supresión del Dato, el artículo 18 señala que los procedimientos para dicho efecto deben incluirse en la política de Tratamiento de información y ser comunicados a los Titulares de los Datos[81]. El artículo 22, por su parte, establece que el Responsable o Encargado del Tratamiento debe adoptar “*las medidas razonables para asegurar que los datos* [sic] *personales que reposan en las bases* [sic] *de datos* [sic] *sean (…) actualizados, rectificados o suprimidos (…)*”[82]. Conforme con esta disposición, y sin necesidad de mayor análisis, es evidente la exigencia de la norma en el sentido de asegurarle al Titular la posibilidad de supresión de sus Datos, pues al tratarse de una obligación legal de resultado, deberá proceder la eliminación definitiva del dato [sic] personal, siempre y cuando sea procedente y permitida por el ordenamiento jurídico.

Con el propósito de dar orientaciones sobre la materia, la Superintendencia de Industria y Comercio expidió el 28 de mayo de 2015 la *“Guía para implementación del principio de responsabilidad demostrada*[83]*(accountability)*[84]”.

El término “*accountability”*[85], a pesar de tener diferentes significados, ha sido entendido en el campo de la protección de Datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, y la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente.
Conforme con ese análisis, las recomendaciones que trae la guía a los obligados a cumplir la Ley 1581 de 2012, son:

---

[80] El texto completo del artículo 27 del Decreto 1377 de 2013 señala: *“Políticas internas efectivas. En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 26 anterior, las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar: 1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable* [sic] *para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este decreto. 2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación. 3. La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento* [sic]*. La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos* [sic] *personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente decreto”.*

[81] El texto completo del artículo 18 del Decreto 1377 de 2013 señala: “*Procedimientos para el adecuado tratamiento* [sic] *de los datos* [sic] *personales. Los procedimientos de acceso, actualización, supresión y rectificación de datos* [sic] *personales y de revocatoria de la autorización* [sic] *deben darse a conocer o ser fácilmente accesibles a los Titulares de la información e incluirse en la política de tratamiento* [sic] *de la información*.”

[82] El texto completo del artículo 22 del Decreto 1377 de 2013 ordena: “*Del derecho de actualización, rectificación y supresión. En desarrollo del principio de veracidad o calidad, en el tratamiento* [sic] *de los datos* [sic] *personales deberán adoptarse las medidas razonables para asegurar que los datos* [sic] *personales que reposan en las bases* [sic] *de datos* [sic] *sean precisos y suficientes y, cuando así lo solicite el Titular o cuando el Responsable haya podido advertirlo, sean actualizados, rectificados o suprimidos, de tal manera que satisfagan los propósitos del tratamiento* [sic]”.

[83] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

[84] *“El término inglés accountability puede ser traducido por rendición de cuentas. Esta voz inglesa, que, en su uso cotidiano, significa ‘responsabilidad’, ha comenzado a emplearse en política y en el mundo empresarial para hacer referencia a un concepto más amplio relacionado con un mayor compromiso de los Gobiernos y empresas con la transparencia de sus acciones y decisiones (…) el término accountability puede ser traducido por sistema o política de rendición de cuentas o, simplemente, por rendición de cuentas (…)”* Recuperado de https://www.fundeu.es/recomendacion/rendicionde-cuentas-y-norendimientomejor-que-accountability-1470/ el 22 de abril de 2019.

[85] Cfr. Grupo de trabajo de protección de datos del artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad, pág. 8.

1. Diseñar y activar un programa integral de gestión de datos [sic] (en adelante PIGDP). Esto, exige compromisos y acciones concretas de los directivos de la organización. Igualmente requiere la implementación de controles de diversa naturaleza;
2. Desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP; y
3. Demostrar el debido cumplimiento de la regulación sobre Tratamiento de Datos personales.

El Principio de Responsabilidad Demostrada –*accountability*- demanda implementar acciones de diversa naturaleza[86] para garantizar el correcto cumplimiento de los deberes que imponen las regulaciones sobre Tratamiento de Datos Personales. El mismo, exige que los Responsables y Encargados del Tratamiento adopten medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia.

Dichas acciones o medidas, deben ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los Datos personales.

El Principio de Responsabilidad Demostrada precisa menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre Tratamiento de Datos personales. Requiere apremiar acciones concretas por parte de las organizaciones para garantizar el debido Tratamiento de los Datos Personales. El éxito del mismo dependerá del compromiso real de todos los miembros de una organización. Especialmente, de los directivos de las organizaciones, pues, sin su apoyo sincero y decidido, cualquier esfuerzo será insuficiente para diseñar, llevar a cabo, revisar, actualizar y/o evaluar los programas de gestión de Datos.

Adicionalmente, el reto de las organizaciones frente al Principio de Responsabilidad Demostrada va mucho más allá de la mera expedición de documentos o redacción de políticas. Como se ha manifestado, exige que se demuestre el cumplimiento real y efectivo en la práctica de sus funciones.

En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que, "*la autorregulación sólo* [sic] *redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que* ***no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento*** [sic] ***indebido de sus datos*** [sic] ***personales****"*[87].(Énfasis añadido).

El Principio de Responsabilidad Demostrada, busca que los mandatos constitucionales y legales sobre Tratamiento de Datos personales sean una realidad verificable y redunden en beneficio de la protección de los derechos de las personas. Por eso, es crucial que los administradores de las organizaciones sean proactivos respecto del Tratamiento de la información. De manera que, por iniciativa propia, adopten medidas estratégicas, idóneas y

[86] Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humana y de gestión. Asimismo, involucran procesos y procedimientos con características propias en atención al objetivo que persiguen.

[87] Cfr. Red Iberoamericana de Protección de Datos. Grupo de trabajo temporal sobre autorregulación y protección de datos personales. Mayo de 5 de 2006. En aquel entonces, la RIPD expidió un documento sobre autorregulación y protección de datos personales que guarda cercana relación con "accountability" en la medida que la materialización del mismo depende, en gran parte, de lo que internamente realicen las organizaciones y definan en sus políticas o regulaciones internas.

suficientes, que permitan garantizar: i) los derechos de los Titulares de los Datos personales y ii) una gestión respetuosa de los derechos humanos.

Aunque no es espacio para explicar cada uno de los aspectos mencionados en la guía[88], es destacable que el Principio de Responsabilidad Demostrada se articula con el concepto de *compliance*, en la medida que este hace referencia a la autogestión o "*conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos*"[89].

También se ha afirmado que, "*compliance es un término relacionado con la gestión de las organizaciones conforme a* [sic] *las obligaciones que le vienen impuestas (requisitos regulatorios) o que se ha autoimpuesto (éticas)"* [90]. Adicionalmente se precisa que, *"ya no vale solo intentar cumplir la ley",* sino que las organizaciones *"deben asegurarse que se cumple y deben generar evidencias de sus esfuerzos por cumplir y hacer cumplir a sus miembros, bajo la amenaza de sanciones si no son capaces de ello. Esta exigencia de sistemas más eficaces impone la creación de funciones específicas y metodologías de compliance*"[91].

Por lo tanto, las organizaciones deben "implementar el *compliance*" en su estructura empresarial con miras a acatar las normas que inciden en su actividad y demostrar su compromiso con la legalidad. Lo mismo sucede con "*accountability*" respecto del Tratamiento de Datos personales.

La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales del *compliance* y buena parte de lo que implica el Principio de Responsabilidad Demostrada (*accountability*). En la mencionada guía se considera fundamental que las organizaciones desarrollen y ejecuten, entre otros, un "*sistema de administración de riesgos asociados al tratamiento* [sic] *de datos* [sic] *personales*"[92] que les permita "*identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales*"[93].

12. RESPONSABILIDAD DE LOS ADMINISTRADORES EN EL TRATAMIENTO DE DATOS PERSONALES.

El artículo 2 de la Constitución Política señala como uno de los fines esenciales del Estado, *"garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución*". De aquí se desprende la exigencia de obtener resultados positivos y concretos del conjunto de disposiciones mencionadas. En este caso en particular, del derecho constitucional a la protección de Datos previsto en el artículo 15 superior.

---

[88] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

[89] Cfr. World Compliance Association (WCA). http://www.worldcomplianceassociation.com/ (última consulta: 6 de noviembre de 2018).

[90] Cfr. Bonatti, Francisco. Va siendo hora que se hable correctamente de compliance (III). Entrevista del 5 de noviembre de 2018 publicada en Canal Compliance: http://www.canal-compliance.com/2018/11/05/va-siendo-hora-que-se-hable-correctamente-de-compliance-iii/

[91] *Idem.*

[92] Cfr. Superintendencia de Industria y Comercio (2015) "*Guía para implementación del principio de responsabilidad demostrada (accountability)*", págs 16-18.

[93] *Ibidem*.

La efectividad de los derechos humanos es un asunto de gran importancia en la sociedad, a tal punto que es una obligación del más alto nivel en el ordenamiento jurídico. Por eso, el artículo 2 continúa ordenando a las "*autoridades de la República (…) proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias, y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares*".

Las normas que hablan de la protección de Datos en el sentido que se estudia, deben ser interpretadas de manera armónica con el ordenamiento jurídico del cual hacen parte y sobre todo con su Constitución Política. Así, su artículo 333 establece que "*la actividad económica y la iniciativa privada son libres, dentro de los límites del bien común*". Este "*bien común*", se refiere a cuestiones relevantes para una sociedad como, por ejemplo, la protección de los derechos humanos, los cuales, son imprescindibles para que cualquier ser humano sea tratado como una persona y no como un objeto.

En línea con lo anterior, la Constitución Política colombiana resalta que la "*libre competencia económica es un derecho de todos que supone responsabilidades*" y que la "*empresa, como base del desarrollo, tiene una función social que implica obligaciones*". Como se observa, la actividad empresarial no puede realizarse de cualquier manera, y en el mundo empresarial no tiene cabida jurídica la afirmación según la cual el fin justifica los medios. En efecto, no se trata de una libertad ilimitada, sino de una actividad responsable y restringida porque no solo debe ser respetuosa del bien común, sino que demanda el cumplimiento de obligaciones constitucionales y legales.

El bien común a que se refiere el artículo 333 mencionado, exige que la realización de cualquier actividad económica garantice, entre otras, los derechos fundamentales de las personas. Es por eso que la Constitución pone de presente que la participación en el mercado supone compromisos y que efectuar actividades empresariales implica cumplir rigurosamente las obligaciones previstas en la ley.

Ahora, según el artículo 22 de la Ley 222 de 1995[94] la expresión administradores comprende al "*representante legal, el liquidador, el factor, los miembros de juntas o consejos directivos y quienes de acuerdo con los estatutos ejerzan o detenten esas funciones*". Cualquiera de ellos tiene la obligación legal de garantizar los derechos de los Titulares de los Datos y de cumplir la Ley 1581 de 2012 y cualquier otra norma concordante. Por esto, el numeral segundo del artículo 23 de la Ley 222 de 1995 determina que los administradores deben "*obrar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios*", y, además, en el ejercicio de sus funciones deben "*velar por* ***el estricto cumplimiento de las disposiciones legales o estatutarias***". (Énfasis añadido).

En vista de lo anterior, la regulación no exige cualquier tipo de cumplimiento de la ley, sino uno calificado. Es decir, ajustado o con exactitud a lo establecido en la norma. Velar por el estricto cumplimiento de la ley exige que los administradores actúen de manera muy profesional, diligente y proactiva para que en su organización la regulación se cumpla de manera real y no formal, con la efectividad y rigurosidad requeridas.

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

---

[94] Ley 222 de 1995 "Por la cual se modifica el Libro II del Código de Comercio, se expide un nuevo régimen de procesos concursales y se dictan otras disposiciones"

El artículo 24[95] de la Ley 222 de 1995, presume la culpa del administrador "*en los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos*". Esta presunción de responsabilidad, exige que los administradores estén en capacidad de probar que han obrado con lealtad y la diligencia de un experto. Es decir, como un "*buen hombre de negocios*", tal y como lo señala su artículo 23.

Adicionalmente, no debe perderse de vista que los administradores responden "*solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros*"[96]. Las disposiciones referidas, prevén unos elementos de juicio ciertos, i) el alto nivel de responsabilidad jurídica y económica en cabeza de los administradores, y ii) el enorme profesionalismo y diligencia que debe rodear su gestión en el Tratamiento de Datos personales.

13. CONCLUSIONES

Sin perjuicio de lo establecido, no se accederá a las pretensiones de la recurrente por, entre otras, las siguientes razones:

1. Las órdenes no son sanciones sino son medidas necesarias para, entre otras, hacer efectivo el derecho al debido tratamiento de datos personales o para que los Responsables del Tratamiento y Encargados del Tratamiento cumplan correctamente los previsto en regulación con miras a garantizar el debido tratamiento de los datos personales y el respeto de los derechos de los Titulares de los datos;

2. No es cierto que la decisión de esta entidad se funda en una norma y/o decisión española. Aunque la investigada tiene derecho a la defensa, ello no debe hacerse recurriendo a afirmaciones que carecen de veracidad. Son inaceptables ese tipo de estrategias de defensa jurídica y de argumentos que faltan a la verdad porque no son correctos ni éticos. Adicionalmente, son irrespetuosos con las autoridades de la República de Colombia;

3. ZOOM VIDEO COMMUNICATIONS, INC emplea diversas tecnologías para recolectar datos personales en el territorio de la República de Colombia, entre las que se incluyen las *web cookies;*

4. El Tratamiento de Datos Personales que realiza Zoom está sujeto a la legislación de la República de Colombia en virtud de la recolección de información de ciudadanos y residentes es este territorio. La Ley Estatutaria 1581 de 2012 es aplicable a ZOOM

---

[95] Artículo 24, Ley 222 de 1995 ""*Responsabilidad de los administradores. El artículo 200 del Código de Comercio quedará así: Artículo 200. Los administradores responderán solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros.*
No estarán sujetos a dicha responsabilidad, quienes no hayan tenido conocimiento de la acción u omisión o hayan votado en contra, siempre y cuando no la ejecuten.
En los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos, se presumirá la culpa del administrador.
De igual manera se presumirá la culpa cuando los administradores hayan propuesto o ejecutado la decisión sobre distribución de utilidades en contravención a lo prescrito en el artículo 151 del Código de Comercio y demás normas sobre la materia. En estos casos el administrador responderá por las sumas dejadas de repartir o distribuidas en exceso y por los perjuicios a que haya lugar.
Si el administrador es persona jurídica, la responsabilidad respectiva será de ella y de quien actúe como su representante legal.
Se tendrán por no escritas las cláusulas del contrato social que tiendan a absolver a los administradores de las responsabilidades antedichas o a limitarlas al importe de las cauciones que hayan prestado para ejercer sus cargos".

[96] Cfr. Parte inicial del artículo 24 de la Ley 222 de 1995.

VIDEO COMMUNICATIONS, INC porque captura Datos Personales por medio de cookies que instala en dispositivos móviles y computadores ubicados en Colombia;

a) Autoridades de protección de datos de varios países -*Uruguay, España, Irlanda, Reino Unido, Italia y Estados Unidos*- y el Tribunal de Justicia de la Unión Europea (TJUE) se han referido a la definición de *"cookies"* y su función. De las mismas se concluye, entre otras: (i) Las *cookies* se instalan en los equipos de las personas (teléfonos celulares, *tablets*, computadoras o cualquier otro dispositivo que almacene información); (ii) La finalidad de las *cookies* es recolectar o almacenar Datos personales (nombre de usuario, un identificador único, dirección de correo electrónico, las búsquedas que realiza de cada usuario y sus hábitos de navegación en internet, sitios que una persona visita en la web) y otros tipos de información; (iii) Las *cookies* son un mecanismo de rastreo o de seguimiento de las personas. Por ejemplo, permiten realizar trazabilidad detallada de las búsquedas de un usuario en internet o de sus hábitos de navegación; (iv) La recolección o almacenamiento de información mediante las *cookies* constituye un Tratamiento de Datos personales.

5. Insostenible e incompatible con la Ley 1581 de 2012 es el argumento de la recurrente, la cual olvida que, entre otras, para recolectar datos en Colombia no es necesario estar domiciliado en este país. Avances y herramientas tecnológicas permiten que empresas u organizaciones recolecten datos en Colombia sin hacer presencia física en nuestro territorio. Estas organizaciones realizan *"presencia tecnológica"* en nuestro país mediante el uso de las citadas herramientas o aplicativos que se instalan en los equipos (teléfonos, tabletas, computadores, etc) de personas ubicadas en el territorio colombiano. Esa realidad no puede desconocerse ni ser argumento para eximirse de la aplicación de la regulación colombiana.

   No es sensato que quien recolecte y trate datos en el territorio de la República de Colombia - *sin estar domiciliado o residir en el mismo* - acuda a argumentos clásicos de territorialidad no solo para para evadir sus responsabilidades legales frentes a las autoridades y los titulares de los datos, sino para desconocer el ámbito de aplicación de la citada ley.

6. ZOOM VIDEO COMMUNICATIONS, INC no deber ahorrar esfuerzos para mejorar los niveles de seguridad que exige la regulación para todos los usuarios de sus servicios. **Sin seguridad no hay debido Tratamiento de Datos personales. Por ende, Zoom debe ser más responsable, diligente y muy profesional con el Tratamiento seguro de los Datos de sus usuarios**.

Así las cosas, una vez analizada toda la actuación administrativa, la información y documentos que conforman el expediente, concluye el Despacho que la resolución objeto de impugnación fue expedida observando la ley.

De esta forma y conforme con lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, se confirmará, en su totalidad, la Resolución No. 74519 de 23 noviembre de 2020.

En mérito de lo expuesto, este Despacho,

RESUELVE

ARTÍCULO PRIMERO. Confirmar en todas sus partes la Resolución No. 74519 de 23 noviembre de 2020, de conformidad con lo expuesto en la parte motiva del presente acto administrativo.

ARTÍCULO SEGUNDO. Notificar personalmente el contenido de la presente resolución a ZOOM VIDEO COMMUNICATIONS, INC a través de su representante legal o su apoderado o quien haga sus veces, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

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

NOTIFÍQUESE Y CÚMPLASE
Dada en Bogotá, D.C., diciembre 23 de 2021

El Superintendente Delegado para la Protección de Datos Personales,

NELSON REMOLINA ANGARITA

Firmado digitalmente por NELSON REMOLINA ANGARITA
Fecha: 2021.12.23 17:51:51 -05'00'

NELSON REMOLINA ANGARITA

MEGD

Notificación

Sociedad: ZOOM VIDEO COMMUNICATIONS, INC
Identificación: Sin identificación
Correo electrónico: nate.cooper@zoom.us
legal@zoom.us
Dirección: N/A
Ciudad: San José, California
País: Estados Unidos de Norteamérica

Apoderado: Mauricio Jaramillo Campuzano
Identificación: C.C. 80.421.942
Tarjeta profesional: 74.555 del Consejo Superior de la Judicatura
Dirección: Calle 67 No. 7-35 Of. 1204
Ciudad: Bogotá
Correo electrónico: mjaramillo@gomezpinzon.com