REPÚBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 54172 DE 2021

(25 AGOSTO 2021)

"Por la cual se resuelve un recurso de reposición y se concede el recurso de apelación"

Radicación 20-087350

VERSIÓN ÚNICA

EL DIRECTOR DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES

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

CONSIDERANDO

PRIMERO: Que mediante 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 para garantizar el debido Tratamiento de datos personales en el territorio de la Republica de Colombia emitió varias ordenes administrativas de **carácter preventivo** a la sociedad **ZOOM VIDEO COMMUNICATIONS, INC (en adelante Zoom).**

Las ordenes administrativas de carácter preventivo que impartió esta autoridad mediante Resolución No. 74519 del 23 de noviembre de 2020 fueron las siguiente:

> **"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 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 radicado 20- 087350- 17 del 22 de enero de 2021, a través de apoderado, la sociedad extranjera presentó escrito en donde solicitaba, "*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*".

TERCERO: Que mediante radicado 20- 087350- 19 del 28 de enero de 2021, a través de apoderado, la sociedad extranjera presentó escrito con el cual interpuso recurso de reposición y en subsidio de apelación contra la Resolución No. 74519 del 23 de noviembre de 2020. En el escrito la sociedad solicita "*revocar la Resolución No. 74519 del 23 de noviembre de 2020, y ordenar el archivo de la actuación administrativa, o modificar el contenido de la Resolución en lo que resulte aplicable conforme los argumentos presentados por Zoom*". Y, en "*caso de que el recurso de reposición sea resuelto en forma desfavorable total o parcialmente, solicito se envíe el expediente al superior jerárquico para el correspondiente trámite del recurso de apelación*". Lo anterior, con fundamento en:

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

El RPDC no se aplica a Zoom porque Zoom, como empresa extranjera, no realiza operaciones de procesamiento de datos personales dentro del territorio colombiano. 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 ningún tratado aplicable).3 El ámbito territorial del RPDC es mucho más restringido que otros regímenes, incluida la Ley Brasileña de Protección General de Datos (Lei Geral de Proteção de Dados, "LGPD")4 y el Reglamento General de Protección de Datos de la Unión Europea ("RGPD").

El alcance limitado del RPDC ha sido reconocido en repetidas ocasiones por el Congreso, por la propia SIC y por juristas. Tres veces en tres años el Congreso ha rechazado enmiendas que habrían permitido la aplicación extraterritorial.6 Por ejemplo, más recientemente (en 2017), el Congreso rechazó una enmienda en virtud de la cual el alcance del RPDC, en particular de la Ley 1581 de 2012, se habría ampliado para abarcar el tratamiento por parte de responsables y encargados "que no residan ni estén domiciliados en el territorio de la República de Colombia", pero que conducen operaciones de tratamiento "a través de internet o de cualquier medio [...] sobre datos personales de personas que residan, estén domiciliadas o ubicadas en el territorio de la República de Colombia".7 Al rechazar esta enmienda, el Congreso confirmó implícitamente que el RPDC no permite tal ejercicio de jurisdicción. Además, 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".8 Algunos doctrinantes están de acuerdo con el Congreso y la SIC, y han opinado que el RPDC rige únicamente para las empresas que operan y procesan datos dentro de Colombia.

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" (énfasis añadido). 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. Véase la Respuesta en su apartado 1(e). Estas afirmaciones siguen siendo verdaderas: Zoom sigue sin tener ninguna filial, sucursal o subsidiaria en Colombia, y no mantiene ningún servidor en Colombia. Esto distingue a Zoom de otras empresas estadounidenses que la SIC ha tratado de regular bajo el RPDC, que se establecieron en Colombia a través de una relación con una filial local. Debido a que Zoom no ha establecido una presencia local en Colombia, el RPDC, y en particular la Ley 1581 de 2012, no permite que la SIC regule las operaciones de tratamiento de datos de Zoom en el extranjero.

Como apoyo a la aplicación del RPDC a las operaciones extranjeras de Zoom, la Resolución cita la sentencia C-748 de 2011 emitida por la Corte Constitucional de Colombia, que sugiere (según la interpretación de la SIC) que un "factor subjetivo" puede justificar la regulación ampliada de las empresas con sede fuera del territorio colombiano. Véase el punto 5 de Resolución (en el que se cita la sentencia C-748 de 2011).11 Sin embargo, como se deja claro en la propia sentencia C-748, y en otras decisiones, el uso de un "factor subjetivo" para ampliar el alcance del RPDC solo es permisible cuando un tratado internacional permite la competencia extraterritorial, sin que ningún tratado aplique en este caso. Incluso en ese caso, una ley puede ampliar su alcance a través del "factor subjetivo" solo cuando el factor decisivo es la identidad de las partes.12 En este caso, conforme al artículo 2 de la Ley 1581 de 2012, la Resolución se centra en un factor objetivo, es decir, la ubicación del tratamiento, en lugar de un factor subjetivo (la identidad de la persona que realiza dicho tratamiento, cuando se aplica un tratado internacional). Por lo tanto, la sentencia C-748 de 2011 no permite a la SIC ejercer jurisdicción sobre el tratamiento de datos de Zoom fuera de Colombia (salvo que un tratado internacional lo permitiera, lo cual no es así).

El intento de la SIC por ejercer jurisdicción sobre Zoom también es contrario al principio de soberanía nacional. La Corte Constitucional de Colombia 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).13 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.

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.

B. El uso de cookies por parte de Zoom no establece jurisdicción

Dado que el RPDC no rige para las actividades de Zoom fuera de Colombia, la Resolución cita el supuesto uso de cookies por parte de Zoom como único fundamento para el ejercicio de su supuesta jurisdicción. Véase las páginas 5 y 6 de la Resolución; véase también la página 20 (que concluye que "La Ley 1581 de 2012 es aplicable a ZOOM VIDEO COMMUNICATIONS, INC porque recolectan Datos personales en el territorio de la República de Colombia a través de cookies que instala en los equipos o dispositivos de las personas residentes o domiciliadas en Colombia"). Pero el intento de la SIC de ejercer jurisdicción sobre Zoom basado en el uso de cookies es contrario al derecho colombiano.

Para empezar, 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. En particular, la legislación colombiana no regula explícitamente las cookies, a diferencia, por ejemplo, de la Unión Europea, donde la Directiva de Privacidad Electrónica14 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. Asimismo, incluso 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.

En cualquier caso, aun si las cookies de Zoom "trataran" datos personales conforme a lo definido en la legislación colombiana, 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. Sobre estos hechos, no es coherente con el debido proceso que la SIC regule a Zoom por su uso de cookies, simplemente porque los usuarios en Colombia (al igual que los usuarios en cualquier parte del mundo) pueden navegar en el sitio web de Zoom, el cual necesariamente requerirá de cookies para operar. Efectivamente, 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.

Además, incluso si el uso general de las cookies por parte de Zoom para alojar un sitio web global pudiera constituir un fundamento para la jurisdicción en Colombia (que, como se explicó, no es el caso), eso no sería un argumento jurisdiccional suficiente para permitir que la SIC regule las prácticas de seguridad de datos personales de Zoom relacionadas con su servicio de reuniones. De hecho, la Resolución menciona las cookies solo en relación con el análisis relativo a su competencia, y no sugiere que las cookies de Zoom sean inadecuadas, ni susceptibles a vulnerabilidades de seguridad, ni que su uso carezca de transparencia. Dado que el Requerimiento de la SIC no se centra en las cookies que intenta utilizar para justificar su jurisdicción, la SIC ni siquiera requirió a Zoom información sobre sus cookies en el Requerimiento, y como resultado, Zoom no tuvo ocasión de responder sobre las cookies en su Respuesta.

(…)

III. LA RESOLUCIÓN ES NULA POR AUSENCIA DEL DEBIDO PROCESO, FALTA DE PRUEBAS Y ANÁLISIS JURÍDICO

Zoom no tiene la obligación de cumplir con las leyes colombianas que rigen el tratamiento de datos personales. Sin embargo, Zoom ha implementado voluntariamente medidas integrales de protección de la seguridad que cumplen plenamente la legislación colombiana. En particular, la Resolución no contiene 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. 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 conclusiones. 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. Debido a estas deficiencias, la Resolución es nula en virtud del artículo 137 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo ("CPACA").

(…)

Las decisiones administrativas deben basarse en el principio fundamental del debido proceso. En particular, una empresa que se enfrenta a acciones administrativas tiene derecho a presentar una defensa adecuada y el derecho a solicitar que las autoridades consideren pruebas que respalden su posición.

En este caso, 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 a ellos y de explicar si describieron con precisión la seguridad de Zoom (lo cual no hacen). 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 (como se mencionó anteriormente), ni incluyó en la Resolución argumentos sobre cómo Zoom utilizaba cookies para procesar datos personales en virtud del RPDC, o en relación con las inquietudes planteadas.

(…)

De conformidad con el artículo 137 del CPACA, un acto administrativo es nulo cuando ha sido expedido mediante falsa motivación, es decir, cuando (a) los hechos que la Administración tuvo en cuenta como motivos determinantes de la decisión no estuvieron debidamente probados; o b) cuando se omite tener en cuenta o se ignoran hechos que sí estaban demostrados y que si hubiesen sido considerados habrían conducido a una decisión sustancialmente diferente.[20] En este caso, ambos son verdaderos: 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.

Además, un acto administrativo debe contener un fundamento jurídico adecuado basado en los hechos constatados. Como explica el tribunal Constitucional[21] y el Consejo de Estado,[22] se requiere más que una sección titulada "consideraciones"; en cambio, los actos de las autoridades colombianas, como la Resolución, deben contener motivaciones suficientes y particulares para justificar la carga impuesta. En este caso, la 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.

(…)

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.

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, Directora de Cumplimiento y Ética (Chief Compliance and Ethics Officer) y Oficial de Privacidad (Chief Privacy Officer) de Zoom. La Sra. Haaland anteriormente fue directora de cumplimiento y ética global y directora jurídica de ciberseguridad en PepsiCo, y se desempeñó durante doce años como fiscal federal.

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. Zoom publicó una declaración de privacidad completa en su sitio web. Como se explicó en la Respuesta, Zoom ha establecido un programa de seguridad mediante el Marco para Mejorar la Ciberseguridad de Infraestructura Crítica (Framework for

Improving Critical Infrastructure Cybersecurity) establecido por el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, "NIST"), de los Estados Unidos, así como el estándar de auditoría "SOC 2" de los controles a los sistemas y organizaciones de servicios (System and Organization Controls, "SOC 2"). Las auditorías SOC2 Tipo 2 regulares de Zoom proporcionan "información detallada y garantía sobre los controles en una organización de servicios relevante para la seguridad, disponibilidad e integridad de procesamiento de los sistemas que la organización de servicios usa para procesar los datos de los usuarios y la confidencialidad y privacidad de la información procesada por esos sistemas." (traducción propia).[24] Zoom también ha adoptado las medidas técnicas de seguridad descritas en su Respuesta (Respuesta 3-4) y descritas más detalladamente en su documento técnico de seguridad (White Paper). Estas medidas organizativas y técnicas satisfarían más que las normas establecidas en la Guía para la implementación del Principio de Responsabilidad Demostrada.

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. Zoom renueva su Certificación SOC2 Tipo 2 cada año. Y, como se explica en su Respuesta, a principios de este año, Zoom promulgó una "congelación de características" (feature freeze) de 90 días durante la cual Zoom centró todos sus recursos de ingeniería en la mejora de la seguridad. Durante esos 90 días, Zoom tomó medidas importantes y concretas para mejorar su (ya sólida) seguridad y satisfacer así las nuevas necesidades identificadas durante la pandemia. Estas medidas concretas incluyeron el lanzamiento de Zoom 5.0, que (entre otras cosas) implementó características técnicas de seguridad diseñadas para mejorar la seguridad de las reuniones.[28] Incluso después de la conclusión del plan de 90 días en julio, Zoom ha seguido demostrando su compromiso con la seguridad al hacer disponible un factor de autenticación múltiple, y mejoramiento adicional de sus parámetros de seguridad. Adicionalmente, los residentes de Colombia se beneficiarán de las medidas de seguridad mejoradas que Zoom implementará con relación al acuerdo suscrito con la FTC. La oferta de servicios y el software de Zoom es consistente (en mayor parte) en las muchas jurisdicciones en donde Zoom opera, incluyendo Colombia. Por lo tanto, las mejores a la seguridad de Zoom beneficiarán a todos los usuarios en cualquier lugar en que se encuentren.

Zoom describió su fuerte programa de seguridad en su Respuesta. La seguridad de Zoom solo se ha hecho más fuerte en los últimos seis meses, y continuará fortaleciéndose mientras Zoom implemente mejoras adicionales en conexión con el acuerdo con la FTC. Sin embargo, la SIC no tuvo en cuenta las pruebas presentadas por Zoom en su Respuesta concerniente a su seguridad, y no dio a Zoom la oportunidad de presentar las pruebas adicionales incluidas aquí que permiten concluir que su seguridad es adecuada. Dado que los términos de la Resolución no son consistentes o complementarios a los compromisos de Zoom en el acuerdo con la FTC, la Resolución impone una carga gravosa que no implicarán necesariamente beneficios a los ciudadanos colombianos. Esta falla de la SIC anula la Resolución en virtud del artículo 137 del CPACA.

(…)

No se produjo ningún incidente de seguridad sobre datos personales como consecuencia de ningún evento denunciado en medios de comunicación, y la Resolución no contiene pruebas de que los datos personales de algún residente colombiano hayan sido alguna vez objeto de adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. No hay pruebas, y la SIC no menciona su existencia, sobre algún daño concreto a ciudadanos colombianos.

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. Véanse páginas 13 a 18 de la Resolución. Sin embargo, 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". Id. en página 21. La Resolución no contiene ninguna prueba efectiva, como análisis técnicos, informes de peritos o evaluaciones de las prácticas reales de seguridad de Zoom, que sería lo pertinente en virtud de la Ley colombiana. Además, la Resolución tampoco establece que los usuarios en Colombia alguna vez hayan sufrido (o enfrenten el riesgo de sufrir) algún daño. El hecho de que se base en esta prueba insuficiente hace que la Resolución sea nula en virtud del artículo 137 del CPACA.

(…)

CONCLUSIÓN

Zoom solicita respetuosamente que se revoque o se modifique la decisión contenida en la Resolución. En primer lugar, el uso que hace Zoom de cookies en su sitio web general y mundial no permiten a la SIC ejercer jurisdicción sobre Zoom en ningún sentido, y mucho menos regular aspectos de las prácticas de seguridad de datos de Zoom que no tienen nada que ver con el uso de dichas cookies. Si la SIC tuviera jurisdicción sobre Zoom en este caso, entonces tendría jurisdicción sobre todos los marcos de seguridad de datos corporativos de cada empresa que tiene un sitio web, esencialmente, en todo el mundo. Tal conclusión es claramente incompatible con la Constitución de Colombia y el RPDC.

La SIC tampoco le dio a Zoom una oportunidad justa de defenderse antes de imponer obligaciones gravosas mediante la orden administrativa. Las únicas pruebas citadas en la Resolución son publicaciones de los medios de comunicación de terceros y las acusaciones irrelevantes del proyecto de reclamación presentado por la FTC. Significativamente, mientras se basa en el procedimiento de la FTC para alegar deficiencias de seguridad, la SIC ignora la parte del acuerdo de conciliación por la cual la FTC indica que el acuerdo de Zoom no es una admisión de ninguna irregularidad. Si se le hubiera dado la oportunidad de hacerlo, Zoom habría sido capaz de abordar en su totalidad cualquier inquietud que la SIC pudiera haber tenido sobre cualquiera de estos temas. Más importante aún, todos los problemas subyacentes denunciados por estos medios de comunicación (problemas que ni siquiera eran vulnerabilidades de seguridad en lo absoluto) se han resuelto desde hace mucho tiempo. La SIC no identifica ningún caso en el que alguno de los temas descritos en los artículos de noticias o el proyecto de reclamación presentado por la FTC haya ocasionado un incidente de seguridad, o la explotación o divulgación de ningún dato personal de usuarios en ninguna parte del mundo, y mucho menos en Colombia. Efectivamente, la Resolución no contiene hallazgos de que los datos personales de cualquier residente colombiano hayan sido alguna vez objeto de adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, o que un solo residente en Colombia haya sufrido cualquier daño concreto.

Los clientes de Zoom confían en él para proveer servicios de videoconferencia seguros. Con el fin de mantener la confianza de sus usuarios, y debido a que es lo correcto, Zoom mejora regularmente su seguridad, al tiempo que responde para abordar nuevas amenazas a medida que se identifican. Como se detalla en este documento, la seguridad de Zoom es robusta y solo se ha hecho más fuerte como resultado de su plan de seguridad de 90 días, y medidas posteriores como la implementación de la autenticación multifactorial y el cifrado mejorado de extremo a extremo. Los imperativos comerciales de Zoom de brindar servicios seguros son tan ciertos en Colombia, como en los Estados Unidos y en otros lugares. Sin embargo, el mero hecho de que Zoom y la SIC compartan el objetivo de garantizar la seguridad de los datos de los usuarios no significa que la SIC sea competente para imponer cargas gravosas de cumplimiento a Zoom. Zoom no tiene operaciones ni actividades de procesamiento de datos en Colombia, y por lo tanto está fuera del alcance del RPDC. Por lo tanto, en el marco del presente recurso de reposición y en subsidio de apelación, Zoom solicita a la SIC a revocar la Resolución o modificarla de acuerdo con lo solicitado en el presente documento".

CUARTO: 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 sociedad recurrente en el escrito de reposición y en subsidio apelación contra la Resolución No. 74519 del 23 de noviembre de 2020, se procede a resolver el recurso de reposición, de acuerdo con las siguientes:

CONSIDERACIONES DE LA DIRECCIÓN DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES

I. NTOFICACIÓN DE LA RESOLUCIÓN NO. 74519 DEL 23 DE NOVIEMBRE DE 2020

Se observa en el expediente que desde el cuatro (4) de diciembre de dos mil veinte el apoderado de la sociedad extranjera le comunicó a esta autoridad que actuaría como apoderado de Zoom en el proceso de la referencia. Lo anterior, en los siguientes términos:

Mauricio Jaramillo Campuzano 4 de diciembre de 2020 a las 15:38
Otorgamiento de poder a Mauricio Jaramillo Campuzano - Proceso 20-87350 ante la Superintendencia de Industria y Comercio de...
Para: contactenos@sic.gov.co, Cc: Mauricio Jaramillo Campuzano Detalles

Señores,
Superintendencia de Industria y Comercio
E.S.D.

Referencia: Resolución 74519 de 2020 emitida bajo el proceso con radicado 20-87350
Asunto: Otorgamiento de poder a Mauricio Jaramillo Campuzano

MAURICIO JARAMILLO CAMPUZANO, mayor de edad, domiciliado en la ciudad de Bogotá, identificado como aparece en el poder adjunto, presento a ustedes el poder (el "Poder") emitido por Zoom Video Communications Inc. (Zoom), conforme a las exigencias legales del Decreto 806 de 2020 y el Código General del Proceso, para efectos de ejercer la representación judicial de Zoom en el proceso de la referencia, conforme a las facultades dispuestas en el Poder adjunto.

Para esos efectos, se adjunta a este correo:

- El Poder emitido por Zoom en calidad de poderdante a favor mío, en calidad de apoderado.
- El Certificado de Good Standing emitido por el estado de Delaware, Estados Unidos de América, que acredita la debida incorporación de Zoom.
- El correo enviado por Zoom con asunto "Autorización Notificación Personal Electrónica" para designar la dirección de correo corporativa nate.cooper@zoom.us como canal para efectuar la notificación personal a la que se refiere la "CITACIÓN NOTIFICACIÓN" enviada por la SIC el 23 de noviembre al correo legal@zoom.us y bajo el radicado 0-87350- -6.
- El correo electrónico con asunto "Otorgamiento de poder a Mauricio Jaramillo Campuzano - Proceso 20-87350 ante la Superintendencia de Industria y Comercio de Colombia" enviado por nate.cooper@zoom.us a mjaramillo@gomezpinzon.com. Que incluye el Poder y el certificado de *Good Standing*, adjuntos.

Se destaca que la dirección de email desde la cual se me envió el poder corresponde con la dirección de correo electrónico corporativa que Zoom pidió registrar ante la SIC el 25 de noviembre de 2020 para efectos de recibir la notificación personal a la que se refiere la "CITACIÓN NOTIFICACIÓN" con radicado 0-87350- -6. Se destaca que a la fecha Zoom no ha sido notificada personalmente a través del envío de la Resolución 74519 de 2020 al correo registrado conforme consta en los documentos adjuntos.

Así mismo, se destaca que a la fecha, ni yo, ni mi poderdante hemos tenido acceso al expediente de la referencia. Por lo tanto, se solicita que se me habilite, a través de las credenciales que constan en los sistemas de la SIC a mi nombre y vinculados con mi correo electrónico, para consultar de forma electrónica el expediente del proceso de la referencia.

Agradezco acusar recibo de este envío.

Cordialmente,

MAURICIO JARAMILLO CAMPUZANO
C.C. 80421942
TP 74555 DEL CSJ

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:

Industria y Comercio
SUPERINTENDENCIA

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

Anexos: 0
Elaboró: SIRLENI ROA

De conformidad con el Decreto 2150 de 1995 y la Resolución 11952 de 2016, la firma mecánica aquí plasmada tiene plena validez para todos los efectos legales. Puede verificar la autenticidad de este documento a través de 'www.sic.gov.co', sección 'Consulte aquí el estado de su trámite' con el número de radicado respectivo.

Señor ciudadano, para hacer seguimiento a su solicitud, la entidad le ofrece los siguientes canales:
www.sic.gov.co – Teléfono en Bogotá: 5920400 – Línea gratuita a nivel nacional: 018000910165
Dirección: Cra. 13 # 27 - 00 pisos 1, 3, 4, 5, 6, 7 Y 10, Bogotá D.C.- Colombia
Teléfono: (571) 5870000 – e-mail: contactenos@sic.gov.co

Nuestro aporte es fundamental,
al usar menos papel contribuimos con el medio ambiente

El futuro es de todos | Gobierno de Colombia

Considerando que solo a partir del día veintiuno (21) del mes de enero el apoderado tuvo acceso al expediente, se allegó una "***Solicitud de medidas correctivas sobre la notificación a Zoom de la Resolución 74519 de 2020***". En dicho documento, el apoderado de Zoom solicita a esta autoridad: "*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*".

Con 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.

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

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

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

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

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

> "***cualquier operación o conjunto de operaciones sobre datos*** *[sic] personales, tales como la* ***recolección****, almacenamiento, uso, circulación o supresión*"[1]. (Destacamos)

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

Nótese que la definición de Tratamiento tiene las siguientes características:

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

Sobre este punto, la Corte Constitucional señaló lo siguiente en el numeral 2.5.9. de la Sentencia C-748 de 2011 "*lo que se pretende con este proyecto es que todas las operaciones* ***o conjunto de operaciones con los datos*** *[sic]* ***personales quede regulada por las disposiciones del proyecto de ley*** *en mención, con las salvedades que serán analizadas en otro apartado de esta providencia*". (Destacamos).

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

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

(iii) En tercer lugar, esta autoridad ha reiterado que la regulación sobre Tratamiento de Datos personales **debe aplicarse al margen de los procedimientos, metodologías o tecnologías que se utilicen para recolectar, usar o tratar ese tipo de información**. La ley colombiana permite el uso de tecnologías para tratar datos, pero, al mismo tiempo, exige que se haga de manera respetuosa del ordenamiento jurídico. **Quienes**

[1] Literal g) del artículo 4.

crean, diseñan o usan "innovaciones tecnológicas" deben cumplir todas las normas sobre Tratamiento de datos personales.

III. ZOOM TIENE LA OBLIGACIÓN DE CUMPLIR LA LEGISLACIÓN COLOMBIANA PORQUE REALIZA UN TRATAMIENTO DE DATOS PERSONALES EN TERRITORIO COLOMBIANO POR MEDIO DE LAS WEB COOKIES

El segundo inciso del artículo 2 de la Ley 1581 de 2012 afirma lo siguiente:

> ***"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".* (Destacamos)

En armonía con lo anterior, la Ley 1581 de 2012 delimita el ámbito de aplicación "*al tratamiento de datos personales efectuado* ***en territorio colombiano*****".** Y, como las web *cookies* son instaladas en dispositivos y equipos ubicados en territorio colombiano por Zoom, el Tratamiento de la información que recolecten y traten por medio de esta tecnología queda supeditada al cumplimiento de la Ley 1581 de 2012.

La recurrente considera que:

> "*El RPDC no se aplica a Zoom porque Zoom, como empresa extranjera, no realiza operaciones de procesamiento de datos personales dentro del territorio colombiano. 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 ningún tratado aplicable). El ámbito territorial del RPDC es mucho más restringido que otros regímenes, incluida la Ley Brasileña de Protección General de Datos (Lei Geral de Proteção de Dados, "LGPD") y el Reglamento General de Protección de Datos de la Unión Europea ("RGPD").*

Frente a lo anterior, en ningún momento se ha interpretado la norma por fuera de lo dicho por la misma. Es la propia legislación la que establece que regulará el Tratamiento efectuado en **territorio colombiano** y, además, es la legislación quien enmarca la recolección de datos personales como una operación sobre los mismos, a saber, un Tratamiento.

En este sentido, es importante entender que las *web cookies* instaladas en los **equipos o dispositivos ubicados en territorio colombiano son una manera de recolectar Datos personales**. Es decir, un Tratamiento de Datos personales que ocurre en territorio colombiano. Por tanto, el Responsable del Tratamiento que emplee las web cookies para la recolección de Datos personales en territorio colombiano 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.

La tecnología de seguimiento de web cookies.

Las cookies son una herramienta para, entre otras, recolectar Datos personales. En este sentido, señala Guerrero que las "*entidades públicas y privadas y particulares se hacen presentes en la Red y* ***recaban igualmente datos de otros a distancia sirviéndose de páginas web, (...) y otras aplicaciones 'invisibles' como cookies*** *o web bugs*"[2]. (Destacamos). Según Morón Lerma, las cookies son "*pequeños programas que identifican al usuario cada vez que entra a un servidor de información y que rastrean sus preferencias*". Precisa la autora que, "*el sucesivo envío de cookies y su conservación permite al emitente lograr una fotografía digital del internauta, conocer su dirección, gustos, preferencias o entretenimientos, pudiendo efectuar un rastreo completo de las actividades del usuario en la red*"[3].

Las cookies han sido catalogadas como "*la principal tecnología de rastreo utilizada para controlar a los usuarios en internet* (...)"[4]. Estas tecnologías son utilizadas para realizar "*operaciones invisibles*" y "tratamientos invisibles"[5] de Datos. En síntesis, en Internet se puede recolectar información de

---

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

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

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

[5] El Grupo de Trabajo del artículo 29 expresó en 1999 su preocupación por "todos los tipos de operaciones de tratamiento informático que se llevan a cabo actualmente en Internet a través del software y del hardware sin el conocimiento del interesado y que, por consiguiente, son "invisibles" para el mismo. Ejemplos típicos de este tipo de tratamiento invisible son el chattering en el nivel HTTP1, los hipervínculos automáticos a terceros, el contenido activo (como Java, ActiveX u otras tecnologías que ejecutan scripts en el cliente) y el mecanismo cookies en su aplicación actual en los navegadores usuales"

personas de cualquier parte del mundo a través de diferentes medios tecnológicos visibles e invisibles, conocidos o no por los Titulares de los Datos personales. Esta captura de información técnicamente puede efectuarse sin que la empresa recolectora de los Datos esté físicamente ubicada en el territorio de la persona respecto de la cual se obtiene la información. De hecho, gracias a las tecnologías las empresas hoy en día tienen más presencia electrónica, que física.

Por su parte resulta imperativo reiterar que Zoom reconoce que usa *cookies* para recolectar Datos en el territorio de la República de Colombia. En efecto, dicha empresa manifiesta que:

> Zoom Video Communications, Inc. («Zoom») y nuestros socios usan cookies o tecnologías similares para analizar tendencias, administrar y seguir los movimientos de los usuarios cuando visitan nuestro sitio web o usan nuestros Productos, y para recopilar información sobre usted: desde dónde accede a nuestro sitio web o Productos y cómo usa nuestros Productos y servicios, y para proporcionarle información sobre los productos de Zoom que podría tener interés en comprar.
>
> ¿Qué son las cookies y cómo las usa Zoom?
>
> Las cookies son pequeños archivos de texto que se colocan en su ordenador los sitios web y servicios que visita o a los que accede. Se usan ampliamente para que los sitios web y servicios operen y funcionen con una mayor eficiencia y para proporcionar información sobre la experiencia de nuestros usuarios durante el uso o interacción con nuestros sitios web, productos, servicios y anuncios. Algunas cookies duran solo el tiempo de su sesión web y caducan cuando sale del navegador; otras cookies pueden durar más tiempo que su sesión web, incluso después de que salga del navegador, por ejemplo, para recordarle cuando regresa a nuestro sitio web. En la tabla siguiente se explican las cookies que Zoom y nuestros socios independientes usan y por qué las usan.

Obtenido de https://zoom.us/es-es/cookie-policy.html

Más aún, la compañía le ofrece a los Titulares de la información una tabla para que puedan entender los diferentes tipos de *cookies* que se emplean por esta. Aquella grafica se presenta a continuación:

Cookies	Tipo	Propósito
Cookies obligatorias	Básicas	Estas cookies son necesarias para habilitar funciones básicas del sitio, como para proporcionar un inicio de sesión seguro y recordar su progreso en un pedido.
	Rendimiento	Zoom utiliza cookies de rendimiento para el equilibrio de cargas con objeto de garantizar que los sitios web y productos se mantengan en funcionamiento y operativos.
Cookies funcionales	Preferencias y configuración	Estas cookies se utilizan para registrar la elección y la configuración de un usuario que permiten a nuestros sitios web y productos funcionar correctamente o que mantienen sus preferencias a lo largo del tiempo y que pueden almacenarse en su dispositivo. Por ejemplo, Zoom guarda preferencias como configuración de idioma, navegador y reproductor multimedia, lo que permite al navegador recordar esta configuración cada vez que regresa al sitio.
	Inicio de sesión y autenticación	Cuando inicia sesión en un sitio web o Producto mediante su cuenta de Zoom, almacenamos un número único de identificación y la hora en que inició sesión en una cookie cifrada en su dispositivo. Esta cookie le permite avanzar de una página a otra en el sitio web sin tener que volver a iniciar sesión nuevamente en cada página. También puede guardar su información de inicio de sesión para no tener que iniciar sesión cada vez que regresa al sitio.
	Análisis	Para ofrecer nuestros productos y mejorar su experiencia de usuario en nuestros sitios web y con nuestros Productos, Zoom usa cookies y otros identificadores para recopilar datos sobre uso y rendimiento. Por ejemplo, usamos cookies para contar el número de visitantes individuales a una página o servicio web o en nuestro blog y para elaborar otras estadísticas sobre las operaciones de nuestros productos. Esto incluye cookies de Zoom y de proveedores de análisis independientes. Usamos la información para compilar informes y ayudarnos a mejorar nuestros sitios web y productos.
Cookies de publicidad	Publicidad en función de intereses	Zoom utiliza cookies para recoger datos sobre su actividad en línea e identificar sus intereses para poder enviar publicidad que le resulte relevante. Puede suspender la recepción de publicidad en función de intereses de Zoom tal como se describe en la sección Cómo controlar las cookies de esta política de cookies y en nuestra Política de privacidad. Los usuarios que opten por no «vender» su información personal, no recibirán publicidad en función de sus intereses por nuestra parte en su dispositivo. Nota: si elige no recibir publicidad en función de intereses, almacenamos su preferencia de no recibir comunicaciones en una cookie en su dispositivo.
	Cookies de redes sociales	Algunos de nuestros sitios web y Productos incluyen fragmentos de código proporcionados por compañías de redes sociales que pueden detectar si ya ha iniciado sesión en una cuenta de redes sociales determinada para poder compartir fácilmente el contenido de Zoom con otros usuarios de redes sociales a través de esa cuenta. Estos fragmentos de código leen cookies configuradas anteriormente por el contenido web de la compañía de redes sociales mientras usted tiene la sesión iniciada y consulta ese tipo de contenido en esos sitios de redes sociales. Las empresas de redes sociales no podrán detectar si ya ha iniciado sesión en una cuenta de red social determinada si desactiva la opción de Cookies de publicidad. Nota: si elige no recibir publicidad en función de intereses, almacenamos su preferencia de no recibir comunicaciones en una cookie en su dispositivo. Integramos vídeos del canal de YouTube de Zoom usando el modo de privacidad mejorada de YouTube. Este modo puede colocar cookies en su ordenador cuando haga clic en el reproductor de vídeo de YouTube. YouTube no almacenará información de cookies de identificación personal para la reproducción de vídeos integrados si desactiva las Cookies de publicidad.

Obtenido de https://zoom.us/es-es/cookie-policy.html

(GRUPO DE PROTECCION DE DATOS DEL ARTICULO 29. 1999. Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware. (5093/98/ES/final. WP 17), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp17es.pdf. . . P 2)

Sin perjuicio de lo mencionado consideramos pertinente referirnos a algunas definiciones de las *cookies* para reiterar que son mecanismos que instala Zoom en los equipos o dispositivos ubicados en territorio de la República de Colombia para recolectar en nuestro país Datos personales:

- La Real Academia de la Lengua Española las define como, pequeños ficheros que se instalan en el disco duro o en el navegador del ordenador, tableta, teléfono inteligente o dispositivo equivalente con funciones de navegación a través de Internet y ayudan, entre otras cosas, a personalizar los servicios del titular de la web, facilitar la navegación y usabilidad a través de ella, obtener información agregada de los visitantes de la web, posibilitar la reproducción y visualización de contenido multimedia en la propia web, permitir elementos de interactuación entre el usuario y la web o habilitar herramientas de seguridad[6].

- La Comisión Federal del Comercio *(Federal Trade Comission[7] – FTC)* define una *cookie* como un pequeño archivo de texto que los sitios web instalan en su computadora. Este organismo también se refiere a los tipos generales de *cookies* que existen:

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

  Cookies persistentes (multi-sesión)
  - ***Permanecen en su computadora y registran información cada vez que usted visita algunos sitios web.***

  Se almacenan en el disco duro de su computadora hasta que usted las elimine manualmente de una carpeta del navegador, o hasta que expiren, que puede ser meses o años después de haber sido instaladas en su computadora (...)"[8]. (Destacamos).

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

  "(...) La instalación y uso de "cookies" sin conocimiento del usuario. *Con frecuencia las redes sociales y plataformas análogas utilizan este tipo ficheros que tienen la posibilidad de almacenar determinada información sobre el usuario y su tipo de navegación a través de un sitio web. Estos ficheros se instalan en los equipos de los usuarios, de forma que resulta posible detectar el lugar desde el que accede el usuario, el tipo de dispositivo empleado (móvil o fijo) para el acceso, el tipo de contenidos accedidos, los lugares más visitados y las acciones habituales realizadas durante la navegación, así como el tiempo empleado en cada una de las páginas, entre otras muchas funcionalidades"[9].*

- El *Berkman Klein Center for Internet & Society* de la Universidad de Harvard, pone de presente que las *cookies* han sido objeto de críticas porque pueden utilizarse como un mecanismo para recopilar de forma invisible información sobre los hábitos de navegación del usuario con fines de *marketing*[10].

---

[6] Recuperado de https://www.rae.es/info/cookies el 25 de noviembre de 2020.

[7] "A cookie is information saved by your web browser. When you visit a website, the site may place a cookie on your web browser so it can recognize your device in the future. If you return to that site later on, it can read that cookie to remember you from your last visit and keep track of you over time". Recuperado de https://www.ftc.gov/site-information/privacy-policy/internet-cookies el 25 de noviembre de 2020.
"A cookie is information saved by your web browser, the software program you use to visit the web. When you visit a website, the site might store a cookie so it can recognize your device in the future. Later if you return to that site, it can read that cookie to remember you from your last visit. By keeping track of you over time, cookies can be used to customize your browsing experience, or to deliver ads targeted to you". Recuperado de https://www.consumer.ftc.gov/articles/0042-online- tracking el 15 de marzo de 2020.
De acuerdo con las anteriores definiciones podría afirmarse que, una cookie es información que se guarda en su navegador web. Esto ocurre cuando, se visita un sitio web, el cual, puede instalar una cookie en su navegador web para que pueda reconocer su dispositivo en el futuro. Así, al regresar a ese sitio virtual, la cookie le permitiría recordarlo a partir de su última visita y realizarle un seguimiento a lo largo del tiempo.

[8] Recuperado de https://www.ftc.gov/es/informacion-sobre-el-sitio/politica-de-privacidad/cookies-de-internet-0 el 25 de noviembre de 2020

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

[10] "Cookies are a mechanism by which a web server and a web browser can jointly "remember" information within or between browsing sessions. The web server sends a cookie containing some information to your browser, which may record it on your hard drive. When you next visit the website, that cookie is sent back to the web server. Cookies are useful because they can be used to improve the user experience. However, cookies have been subject to criticism because they can be used as a mechanism for invisibly gathering information about user's browsing habits for marketing purposes". Recuperado de https://cyber.harvard.edu/about/privacy-policy el 27 de noviembre de 2020.

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

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

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

En suma, se concluye por parte de esta autoridad que, sin lugar a duda, 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.

IV. DEL PRINCIPIO Y DEL DEBER DE SEGURIDAD EN EL DEBIDO TRATAMIENTO DE DATOS PERSONALES.

Sin seguridad no existe debido tratamiento de datos personales. Es por eso que la regulación señala, entre otras, lo siguiente:

Literal g) Artículo 4 de la Ley 1581 de 2012:

> *La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*

Literal d) Artículo 17 de la Ley 1581 de 2012:

> *Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*

Nótese que **la redacción del principio de seguridad tiene un criterio eminentemente preventivo**, lo cual obliga a los Responsables a adoptar medidas apropiadas y efectivas para **evitar** afectaciones a la seguridad de la información sobre las personas.

La relevancia y alcance del deber de seguridad ha sido puesto de presente en los siguientes términos:

> *"La seguridad es un proceso dinámico en constante evolución y prueba. Se quiere que exista un nivel de seguridad apropiado en las diferentes etapas del tratamiento de datos personales en donde las medidas de seguridad sean objeto de evaluación y revisión.*
>
> *Dichas medidas deben estar enfocadas para mitigar los siguientes riesgos: acceso no autorizado a los datos personales, pérdida, destrucción (accidental o no autorizada), contaminación (por virus informático) uso fraudulento, consulta, copia, modificación, adulteración, revelación, comunicación, o difusión no autorizados.*
>
> *Para establecer las medidas se deben tener en cuenta, entre otras, las técnicas de seguridad existentes en general y para sectores específicos, los riesgos que presente el tratamiento y la naturaleza de los datos que deban protegerse, la probabilidad y severidad del daño obtenido, la sensibilidad de la información y el contexto en el que es realizado el tratamiento y las eventuales consecuencias negativas para los titulares de los datos.* (...)
>
> *Proteger la información es una condición crucial del tratamiento de datos personales. Una vez recolectada debe ser objeto de medidas de diversa índole para evitar situaciones indeseadas que pueden afectar los derechos de los titulares y de los mismos Responsables y Encargados*

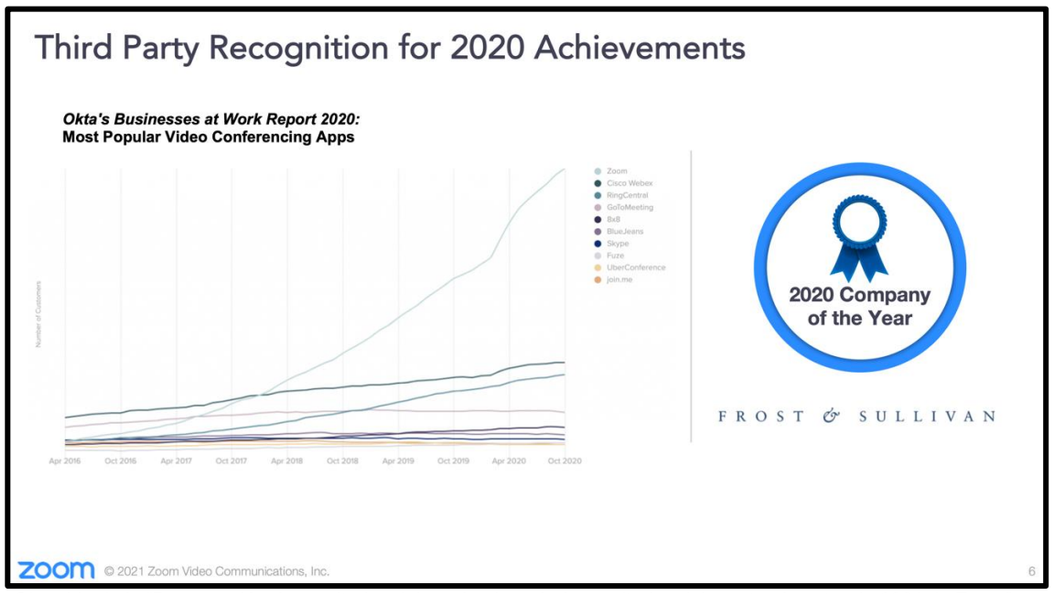
del tratamiento de los datos. El acceso, la consulta y el uso no autorizado o fraudulento así como la manipulación y pérdida de la información son los principales riesgos naturales y humanos que se quieren mitigar a través de medidas de seguridad de naturaleza humana, física, administrativa o técnica"[11].

Por su parte, la Corte Constitucional ha establecido que:

"*Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*
(..)
Existe entonces un deber tanto de los Responsables como los Encargados de establecer controles de seguridad, de acuerdo con el tipo de base de datos que se trate, que permita garantizar los estándares de protección consagrados en esta Ley Estatutaria."[12]. (Subrayado fuera de texto).

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

No debe perderse de vista que, Zoom es una plataforma con gran número de usuarios en el mundo y en la República de Colombia[13]. Pues, en efecto, en el seminario web sobre ganancias del tercer trimestre de 2021 de Zoom, la compañía anunció que el número de actas de reuniones anuales en Zoom supera los 3,3 billones[14]. Más aún, es la propia compañía quien destaca lo siguiente del "*Informe de negocios en el trabajo de Okta 2020: Aplicaciones de videoconferencia más populares*":

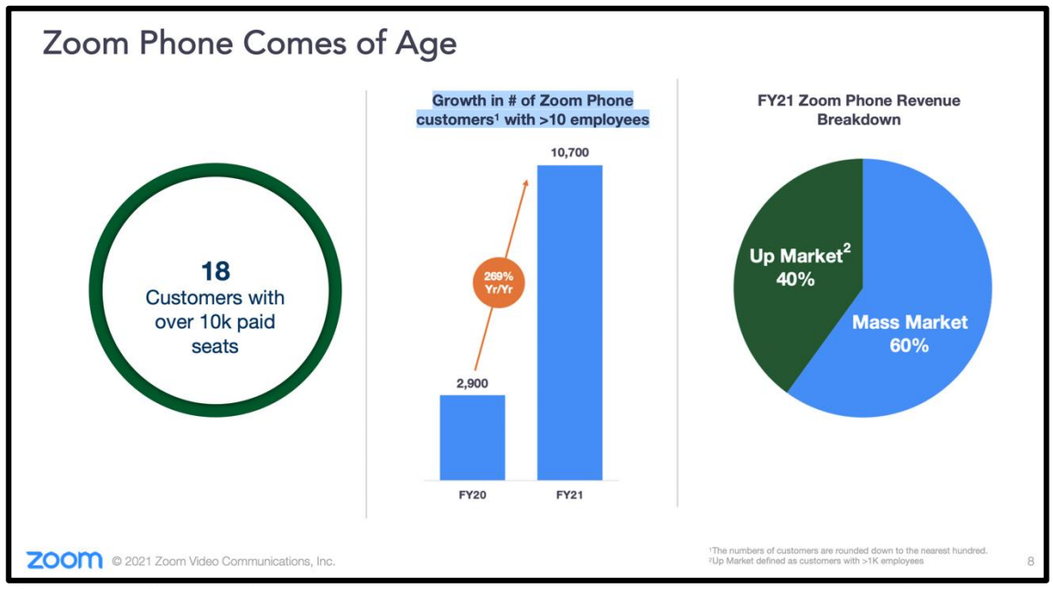


Obtenido de la "Presentación de resultados del seminario web de resultados del cuarto trimestre de 2021 de Zoom" en https://investors.zoom.us/static-files/0e5bc6bc-c329-4004-a20b-99b67714e7b8

En adición, Zoom reportó un incremento en el número de clientes (con más 10 empleados) de "*Zoom Phone*" en aproximadamente 269%. Lo siguiente, según se puede observar:

---

[11] fr. REMOLINA ANGARITA, Nelson. 2013. Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012. 1 ed. Bogotá: Legis Editores. Págs. 216-217
[12] Corte Constitucional. Sentencia C – 748 del 2011.
[13] En Colombia se realizaron 17 millones de reuniones entre el 1 y el 28 de abril de 2020.
[14] Información consultada en https://investors.zoom.us/news-events/events el 3 de agosto de 2021.



Obtenido de la "Presentación de resultados del seminario web de resultados del cuarto trimestre de 2021 de Zoom" en https://investors.zoom.us/static-files/0e5bc6bc-c329-4004-a20b-99b67714e7b8

Se reitera que, la orden impartida es de carácter **preventivo,** para evitar que se afecte la seguridad de los Datos de los colombianos. La misma se adoptó teniendo en cuenta, entre otros, los hechos; investigaciones; actuaciones y conclusiones de Autoridades de Protección de Datos.

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

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

La regulación colombiana sobre Tratamiento de datos le impone al Responsable del Tratamiento el deber demostrar que ha adoptado medidas efectivas para cumplir la ley (Deber de Responsabilidad demostrada). Esto se deriva de lo expresamente señalado en el Decreto 1377 de 2013 que ordena lo siguiente:

> "*Artículo 26. Demostración. Los responsables del tratamiento de datos personales* ***deben ser capaces de demostrar****, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este decreto (…)".* (Destacamos y subrayamos).

Sobre este punto, en la Sentencia C-32 del 18 de febrero de 2021 la Corte Constitucional reiteró lo anterior en los siguientes términos:

> *"219. El principio de responsabilidad demostrada, conocido en el derecho comparado como accountability en la protección de datos personales, es incorporado por la legislación interna por el Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2013. El artículo 26 de esa normativa determina que* ***los responsables del tratamiento de datos personales deberán demostrar, a petición de la Superintendencia de Industria y Comercio****, entidad que obra como autoridad colombiana de protección de datos, que han implementado medidas apropiadas y efectivas para cumplir con las citadas normas jurídicas. (…)*
>
> *"El principio de responsabilidad demostrada, de acuerdo con lo expuesto, consiste en el deber jurídico del responsable del tratamiento de* ***demostrar ante la autoridad de datos que cuenta con la institucionalidad y los procedimientos para garantizar las distintas garantías del derecho al habeas data****, en especial, la vigencia del principio de libertad y las facultades de conocimiento, actualización y rectificación del dato personal."*
>
> *(…)*
>
> *"****el principio de responsabilidad demostrada no se opone a la Constitución, sino que, antes bien, es desarrollo propio de la eficacia del derecho al habeas data*** *(…)"* (Destacamos)

No debe perderse de vista que a pesar de que el campo de acción de Internet desborda las fronteras nacionales, para la Corte Constitucional el nuevo escenario tecnológico y las actividades en Internet no se sustraen del respeto de los mandatos constitucionales.

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

La realidad socio tecnológica del Siglo XXI nos pone de presente la migración del mundo físico y fronterizo al "ciberespacio", el cual se caracteriza por ser tecnológico y sin fronteras geográficas.

Existen diversas referencias sobre lo que significa el ciberespacio. El 8 de febrero de 1996, por ejemplo, se hizo pública la Declaración de Independencia del Ciberespacio[15] en la cual se utilizaron expresiones como "*el nuevo hogar de la mente*" y un "*espacio social global*" en construcción para referirse al mismo. Allí, también se señaló que el ciberespacio no está dentro de las fronteras de los actuales gobiernos, ya que es un mundo inmaterial que "*está a la vez en todas partes y en ninguna parte*".

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

Para el Profesor Lessig, el ciberespacio hace alusión a una "*nueva sociedad*" que surgió en los países occidentales en la "*mitad de la década de los años noventa*". En un principio en "*las universidades y centros de investigación*", y luego en la sociedad en general. Internet es esa nueva sociedad a la que se refiere dicho autor, la cual gira en torno a una "*estructura abierta y de finalidad múltiple de las redes basadas en la transferencia de paquetes de datos (...) en la que cada persona podría ejercer como su propio redactor-jefe y publicar lo que desease*"[16].

En el caso de la regulación colombiana[17], la Comisión de Regulación de Comunicaciones (CRC) incorporó la siguiente definición en el numeral 9 del artículo 1 de la Resolución No. 2258 de 23 de diciembre de 2009[18]: "*Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios*".

En la exposición de motivos de dicha norma se destaca que,

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

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

---

[15] Esta declaración es un texto presentado por John Perry Barlow en Davos (Suiza), confundador de la Electronic Frontier Foundation (https://www.eff.org/). No se trata de un instrumento jurídico vinculante sino de un manifiesto que buscaba que los gobiernos no interfirieran en lo que sucede en internet. El texto puede consultarse en: https://projects.eff.org/~barlow/Declaration-Final.html Última consulta: octubre 20 de 2014)

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

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

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

Aunque existen diferentes acepciones sobre el ciberespacio, consideramos relevante tener presente que el mismo está integrado por los siguientes elementos[19]:

i. Una infraestructura tecnológica (recursos tecnológicos) conformada por un sinnúmero de equipos (servidores, computadores, teléfonos móviles, tabletas, entre otras) que se encuentran ubicados en muchas partes del mundo.
ii. Una plataforma de comunicaciones (red global de comunicaciones), información y redes interconectadas (Internet) de alcance mundial denominada *"infraestructura global de información"*[20].
iii. Millones de personas de diversas nacionalidades, domiciliadas en países con sistemas jurídicos disímiles que desde cualquier parte hacen uso de la tecnología, las comunicaciones y la información para interactuar con otras personas o utilizar los servicios disponibles en Internet.

El ciberespacio ha sido caracterizado por ser un escenario global no delimitado por fronteras geográficas[21] en donde las actividades suceden dentro de la arquitectura tecnológica de Internet. Acá no existe un espacio físico definido (como nuestra casa o el territorio de nuestro país) sino un campo artificial o virtual e indeterminado en donde las personas interactúan. Buena parte de esas actuaciones en el mundo virtual tienen implicaciones y consecuencias jurídicas en el mundo real.

En suma, el ciberespacio hace alusión a un ámbito imaginario, intangible e invisible - en contraposición al mundo real y físico- en donde tienen lugar una serie de acontecimientos que suceden en Internet. Y, aunque se trata de un "mundo virtual", sus ciudadanos son miles de millones de personas reales ubicadas en prácticamente cualquier lugar del "mundo físico" cuyas actividades tienen impacto o consecuencias en el "mundo real"[22].

Ahora bien, en 2001 la Corte Constitucional de la República de Colombia se pronunció sobre, entre otros, el alcance del ordenamiento constitucional frente a la regulación de materias ligadas al ejercicio de actividades a través de Internet[23]. Para la Corte, la información es muy importante y cumple un rol central "*en el funcionamiento de la sociedad actual" e Internet ha sido, entre otros, un escenario en el cual operan muchos "sistemas de información y almacenamiento informático*".

De entrada, la Corte rápidamente advierte sobre lo que sucede con la información que es recolectada en el "mundo virtual" –ciberespacio-. En este sentido, manifiesta que,

> "(…) *la información que se comparte en Internet deja una huella que, por ejemplo, no solo permite establecer el contenido exacto de la transacción comercial efectuada entre un usuario del sistema y el agente material de una actividad que se desarrolla por esta vía (...) sino que, hace posible rastrear e identificar todo lo que una persona hizo en el* ***mundo virtual****, los lugares que visitó o consultó y los productos que consumió a través de la red.* ***La recopilación de estos Datos puede ser utilizada para crear perfiles*** *sobre los gustos, preferencias, hábitos de consulta y consumo de las personas que emplean Internet (como simples usuarios o como agentes económicos que desarrollan sus actividades por este medio*)"[24]. (Negrilla ausente en el original).

De otra parte, la Corte también reconoció la importancia "*que tienen dentro de un sistema global de comunicaciones, como Internet, derechos y libertades tan importantes para la democracia como (...) la intimidad y el habeas data (artículo 15 C.P.)*"[25]. Adicionalmente, dicha corporación admitió que los avances científicos y tecnológicos "***siempre han planteado retos al derecho***" porque éstos inciden, entre otros, "*en el ejercicio de los derechos fundamentales de las personas" y por ende "****demandan diferentes respuestas del ordenamiento jurídico***"[26]. (Énfasis añadido).

---

[19] Sobre algunas características del ciberespacio y los retos que genera al Derecho véase: JOHNSON, David y POST, David. 1995-1996. Law and borders: the rise of law in cyberspace. Stanford Law Review 48:1367-1402.
[20] Reidenberg se refiere a ella como "the global information infrastructure –GII-" (REIDENBERG, Joel R. 1996. Governing networks and cyberspace rule-making. Emory Law Journal 45. p 912)
[21] Cfr. GILDEN, Michael. 2000. Jurisdiction and the internet: the real world meets cyberspace. ILSA Journal of International & Comparative Law 7 (1). P 150.

[22] De hecho, autores como Baronti, han afirmado que el ciberespacio es en últimas una "una proyección simbólica del mundo real" (Cfr. BARONTI, Hugo. 2014. ¿Qué es el ciberespacio?. En: http://baronti.net/textos/292-¿que-es-el- ciberespacio.html (última consulta: octubre 22 de 2014).
[23] Cfr. Corte Constitucional. Sentencia C-1147 del 31 de octubre de 2001. MP. Dr. Manuel José Cepeda Espinosa.
[24] Todas las partes o frases señaladas entre comillas son tomadas de la Sentencia C-1147 de 2001.
[25] Los otros derechos importantes que cita el alto tribunal son: el derecho a la igualdad ; la libertad de conciencia o de cultos; la libertad de expresión; el libre ejercicio de una profesión u oficio; el secreto profesional y el ejercicio de los derechos políticos que permiten a los particulares participar en las decisiones que los afectan (Corte Constitucional, C- 1147 de 2001).
[26] Todas las partes o frases señaladas entre comillas son tomadas de la Sentencia C-1147 de 2001.

A pesar de que el campo de acción de Internet desborda las fronteras nacionales, para la Corte Constitucional el nuevo escenario tecnológico y las actividades en Internet no se sustraen del respeto de los mandatos constitucionales[27]. Por eso, concluye dicha entidad que,

> "***en Internet (...) puede haber una realidad virtual pero ello no significa que los derechos, en dicho contexto, también lo sean****. Por el contrario, no son virtuales:* ***se trata de garantías expresas por cuyo goce efectivo en el llamado "ciberespacio"*** *también debe velar el juez constitucional". Recalca dicha Corporación que, "****nadie podría sostener que, por tratarse de Internet, los usuarios sí pueden sufrir mengua en sus derechos constitucionales***"[28]. (Negrilla ausente en el original).

VI. DE LA FACULTAD LEGAL PARA IMPARTIR LAS ORDENES CONTENIDAS EN LA RESOLUCIÓN NO. 74519 DEL 23 DE NOVIEMBRE DE 2020

En el recurso interpuesto se argumentó que esta entidad no tiene las facultades legales para imponerle a Zoom las órdenes impartidas mediante la Resolución No. 74519 del 23 de noviembre de 2020.

La afirmación de la recurrente es contraria a Derecho porque la Ley Estatutaria 1581 de 2012 expresamente facultad a esta entidad a emitir órdenes o impartir instrucciones necesarias para que el Tratamiento de Datos personales se realice conforme con la ley. En el artículo 19 de esa ley, se le otorgó competencia a esta entidad, a través de la Delegatura para la Protección de Datos Personales, para ejercer: "*(...) la vigilancia necesaria para garantizar que en el tratamiento* [sic] *de datos* [sic] *personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley.*"

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

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

Visto lo anterior, contrario a lo afirmado por Zoom, sí existen expresas y suficientes facultades legales para que esta Superintendencia pueda impartir las ordenes contenidas en la Resolución No. 74519 del 23 de noviembre de 2020.

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".* (Destacamos).

En suma, 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, esta entidad ha sido respetuosa del principio de legalidad y ha obrado conforme con lo establecido en el derecho colombiano.

---

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

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

VII. LA SUPERITENDENCIA DE INDUSTRIA Y COMERCIO GARANTIZÓ EN TODO MOMENTO EL DEBIDO PROCESO

En el escrito bajo estudio, la recurrente afirma que, en relación con las garantías procesales, esta entidad no le otorgó una oportunidad adecuada para hacer declaraciones de defensa frente a la Resolución No. 74519 del 23 de noviembre de 2020. Y debido a esto, esta superintendencia vulneró su derecho al debido proceso.

El inicio de esta investigación fue debidamente informado a la recurrente y ella se pronunció al respecto dando cumplimiento al inciso segundo del artículo 35 de la Ley 1437 de 2011:

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

Siendo así, la comunicación[29] enviada le permitió a Zoom no solo conocer que se estaba desarrollando una investigación administrativa en su contra, también, garantizar su derecho de defensa y contradicción.

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

A su vez, en cumplimiento del artículo 36 de la Ley 1437 de 2011, el expediente digital 20-087350 en todo momento, y desde el inicio de la investigación ha estado a disposición de la sociedad recurrente, para que sea consultado o se pronuncie sobre cualquier aspecto de este. Así como también, ha tenido la posibilidad de presentar oposiciones y de aportar y/o solicitar la práctica de las pruebas que considere pertinentes.

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

> "La jurisprudencia constitucional define el derecho a la defensa como la **'oportunidad reconocida a toda persona**, en el ámbito de cualquier proceso o actuación judicial o **administrativa**, de ser oída, de hacer valer las propias razones y argumentos, de controvertir, contradecir y objetar las pruebas en contra y de solicitar la práctica y evaluación de las que se estiman favorables, así como ejercitar los recursos que la ley otorga'"[30]. (Destacamos).

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

- Luego del inicio de la investigación administrativa que culminó con la expedición de la Resolución No. 74519 del 23 de noviembre de 2020, era decisión de la sociedad recurrente manifestarse en el sentido que prefiriera. Como también, aportar y/o solicitar la práctica de pruebas que considerara relevantes para el desarrollo de la investigación. Para este efecto, el expediente siempre estuvo a disposición de Zoom.
- Los derechos de defensa y contradicción otorgan unas potestades a sus titulares, las cuales no son obligatorias, sino que, parten de la autonomía privada de cada uno de ellos.
- La poca acción procesal de Zoom hasta antes de la expedición de la Resolución No. 74519 del 23 de noviembre de 2020, pese a que se le informó del inicio de la actuación administrativa, además de que siempre tuvo acceso al expediente, no significa que esta entidad haya vulnerado sus derechos o que hubiese actuado de manera ilegal.
- Zoom siempre tuvo oportunidad de expresar sus opiniones y de acceder al expediente. De igual manera, es libre de definir sus estrategias jurídicas y obrar conforme con las mismas. No obstante, si los resultados de la actuación administrativa no son los deseados por esa sociedad, no es dable endilgarle tal responsabilidad a esta entidad, y tampoco afirmar que la misma obró contrario a derecho.

Adicionalmente, los recursos de reposición y apelación interpuestos contra la resolución mencionada son las formas establecidas por la Ley 1437 de 2011 para debatir las conclusiones del acto

---

[29] Comunicación remitida el 14 de abril del 2020 con el radicado 20-87350-0.

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

administrativo definitivo que pone fin a la investigación en curso. Esta posibilidad está en el artículo 74 de la Ley 1437 de 2011:

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

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

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

Entonces, la Superintendencia de Industria y Comercio obró dentro del marco de sus facultades legales para, de una parte, garantizar a las personas el Derecho Fundamental de la Protección de Datos Personales y, de otra, respetar el debido proceso en cabeza de Zoom.

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

Esta autoridad aplicó y respetó las garantías procesales necesarias, y emitió el acto administrativo a que hubo lugar. El que, en ninguna circunstancia fue arbitrario. Por el contrario, lo que sí hizo esta autoridad, fue propender por la correcta aplicación de las normas y los principios que las fundamentan.

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

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

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

Se reitera que esta autoridad:

1. Comunicó el inicio de la investigación a Zoom;
2. Garantizó el derecho de la sociedad a ser oída, aportar y solicitar pruebas; y
3. Garantizó el derecho de contradicción, con el análisis del recurso en cuestión.

VIII. CONTEXTO DE LA ORDEN IMPARTIDA

La Superintendencia de Industria y Comercio ordenó a Zoom adoptar nuevas medidas y mejorar las existentes para garantizar la seguridad de los Datos personales de todos los Titulares que usan la aplicación de video conferencia en el territorio colombiano. Que, según información otorgada por la compañía, en Colombia se realizaron 17 millones de reuniones entre el 1 y el 28 de abril de 2020. La decisión se tomó mediante la Resolución No. 74519 del 23 de noviembre de 2020.

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

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

- Hurto de credenciales desde la aplicación de escritorio Zoom para Windows.
- Transferencia de información a la compañía Facebook.
- Acceso a los perfiles de LinkedIn.

La SIC no solo tuvo en cuenta las publicaciones de los medios de comunicación sino también, las declaraciones de la compañía en sus diversos portales web y las decisiones; solicitudes e informes emitidos por la Comisión Federal de Comercio de los Estados Unidos de Norteamérica.

En primer lugar, Zoom no le demostró a la autoridad la adopción de medidas de seguridad suficientes y efectivas para impedir que los Datos de sus usuarios fueran accedidos y compartidos por un tercero,

en contravía de la normatividad de protección de Datos personales en diferentes países y sus políticas de privacidad.

Finalmente, se puso de presente como 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.** Dicha autoridad sostuvo que Zoom incumplió la obligación de proteger la información de los usuarios de diversas maneras, las cuales se ponen de presente:

- **Zoom dijo que proporcionó codificación punto a punto** — una manera de proteger las comunicaciones para que únicamente las vean el emisor y el receptor — **para las reuniones de Zoom. No lo hizo**.
- **Zoom dijo que protegió las reuniones con un nivel de codificación más alto del que realmente ofreció**.
- Zoom les dijo a los usuarios que grabaron una reunión que, una vez terminada, se guardaría una grabación segura y codificada de esa reunión. En realidad, **Zoom guardó grabaciones sin codificar en sus servidores hasta por 60 días antes de pasarlas a su nube de almacenamiento segura**.
- **Zoom instaló un software, llamado ZoomOpener, en las computadoras Mac de los usuarios. Este programa eludió una función de seguridad del navegador Safari** y puso en riesgo a los usuarios — por ejemplo, podría haber permitido que extraños espiaran a los usuarios a través de las cámaras web de las computadoras. O los piratas informáticos podrían haber explotado la vulnerabilidad para descargar programas maliciosos en las computadoras de los usuarios y tomar el control de sus dispositivos. **Si los usuarios eliminaban la aplicación de Zoom, el programa ZoomOpener permanecía instalado, al igual que estas vulnerabilidades de seguridad**. Zoom podía volver a instalar la aplicación sin el permiso del usuario y sin informárselo.
- Zoom no les contó la historia completa del programa ZoomOpener a los usuarios. **Zoom dijo que el software era una corrección de fallo, pero no les dijo a los usuarios que instalaría un servidor web que circunvalaría una salvaguarda de privacidad y seguridad, o que el software permanecería instalado en sus computadoras incluso después de haber eliminado Zoom**.

En su escrito de reposición, Zoom argumenta que "(…) ***el acuerdo con la FTC*** *es un acto voluntario firmado por Zoom que no implica la admisión de responsabilidad o culpa, que* ***aún no ha sido finalizado y que todavía está sujeto a comentarios públicos*** *(…)"*. Precisamente, el 1 de febrero la citada autoridad finalizó el acuerdo con Zoom Video Communications, Inc., por acusaciones de engaño a los consumidores sobre el nivel de seguridad que se brindaba en las reuniones de la plataforma[31].

La orden final requiere, entre otras, que Zoom:

- Implemente un programa de seguridad integral;
- Revise las actualizaciones de software en busca de fallas de seguridad antes de su lanzamiento; y
- Se asegure de que las actualizaciones no obstaculicen las funciones de seguridad de terceros.

De igual forma, Zoom debe obtener evaluaciones periódicas de su programa de seguridad por parte de un tercero independiente (aprobado por Comisión Federal De Comercio De Los Estados Unidos De América) y notificar a la Comisión si experimenta una brecha de seguridad[32].

Con esto en mente, se observan semejanzas entre las ordenes que se le fueron impartidas a la recurrente por la Superintendencia de Industria y Comercio con aquellas que fueron acordadas con la Comisión Federal De Comercio De Los Estados Unidos De América. A continuación se ponen de presente algunas de aquellas similitudes:

Órdenes impartidas por Superintendencia de Industria y Comercio	**Obligaciones contenidas en el acuerdo final de la Comisión Federal De Comercio**
"Desarrollar, implementar y mantener un programa de gestión y manejo de incidentes de seguridad en Datos personales"[33]	Implementar un programa de gestión de vulnerabilidades[34].

[31] Obtenido de https://www.ftc.gov/news-events/press-releases/2021/02/ftc-gives-final-approval-settlement-zoom-over-allegations-company el 6 de agosto del 2021.
[32] Información obtenida de Decision and Order Docket Nº. C-4731 en https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf el 6 de agosto del 2021.
[33] Resolución No. 74519 del 23 de noviembre de 2020
[34] Traducción de la Información obtenida en Decision and Order Docket Nº. C-4731 en https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf el 6 de agosto del 2021.

"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"[35]	Evaluar y ajustar el Programa a la luz de cualquier cambio en las operaciones de Zoom[36].
"Desarrollar, implementar y mantener un programa de capacitación y entrenamiento rutinario para sus empleados y contratistas sobre su política de seguridad de la información"[37].	Programas regulares de capacitación en seguridad, al menos una vez al año, que se actualizan, según corresponda, para abordar los riesgos internos o externos identificados por Zoom[38].
"Efectuar una auditoría independiente"[39]	Evaluaciones independientes del programa por un tercero[40].

Entonces, como se ha venido reiterando, sin seguridad no hay un debido Tratamiento de Datos personales. Por eso, para esta autoridad, Zoom tiene la enorme responsabilidad de garantizar la seguridad de la información de todos sus usuarios, lo cual la obliga a ser extremadamente diligente en esta labor y a no ahorrar esfuerzos para responder por la seguridad de los Datos de miles de millones de personas.

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

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

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

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

X. 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*"[41].

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.

---

[35] Resolución No. 74519 del 23 de noviembre de 2020
[36] Traducción de la Información obtenida en Decision and Order Docket Nº. C-4731 en https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf el 6 de agosto del 2021.
[37] Resolución No. 74519 del 23 de noviembre de 2020
[38] Traducción de la Información obtenida en Decision and Order Docket Nº. C-4731 en https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf el 6 de agosto del 2021.
[39] Resolución No. 74519 del 23 de noviembre de 2020
[40] Traducción de la Información obtenida en Decision and Order Docket Nº. C-4731 en https://www.ftc.gov/system/files/documents/cases/1923167_c-4731_zoom_final_order.pdf el 6 de agosto del 2021.
[41] Cfr. Corte Constitucional, sentencia T-227 de 2003.

El artículo 26[42] -*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 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]."[43]

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[44]. 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 (…)*"[45]. 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*[46]*(accountability)*[47]".

El término "*accountability*"[48], 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

---

[42] 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"*

[43] 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".*

[44] 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*."

[45] 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]".

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

[47] *"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.

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

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:

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[49] 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****"* [50]. (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 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[51], 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*"[52].

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*

---

[49] 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.
[50] 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.
[51] El texto de la guía puede consultarse en: http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf
[52] Cfr. World Compliance Association (WCA). http://www.worldcomplianceassociation.com/ (última consulta: 6 de noviembre de 2018).

que se ha autoimpuesto (éticas)"[53]. 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*"[54].

Por 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*"[55] 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*"[56].

QUINTO: Sin perjuicio de todo lo anterior, destacamos las siguientes **CONCLUSIONES**:

- La regulación sobre Tratamiento de Datos personales **debe aplicarse al margen de los procedimientos, metodologías o tecnologías que se utilicen para recolectar**, usar o tratar ese tipo de información. La ley colombiana permite el uso de tecnologías para tratar datos, pero, al mismo tiempo, exige que se haga de manera respetuosa del ordenamiento jurídico. **Quienes crean, diseñan o usan "innovaciones tecnológicas" deben cumplir todas las normas sobre Tratamiento de datos personales**.
- Zoom tiene la obligación de cumplir la legislación colombiana porque realiza un Tratamiento de Datos Personales en territorio colombiano por medio de las web *cookies*.
- **La redacción del principio de seguridad tiene un criterio eminentemente preventivo**, lo cual obliga a los Responsables a adoptar medidas apropiadas y efectivas para **evitar** afectaciones a la seguridad de la información sobre las personas.
- **Una empresa tan determinante en la ciberseguridad del mundo como lo es Zoom, en razón de la cantidad de información que maneja, tiene el deber de ser más que diligente en el Tratamiento de Datos personales**, a fin de garantizar la protección de las personas y su privacidad.
- Esta entidad no desconoció el debido proceso para emitir una orden de naturaleza preventiva. **La orden emitida es de carácter preventivo, no se trata de una sanción por causar daños a los Titulares de Datos ubicados en el territorio de la República de Colombia**. Debe recordarse que la mejor forma de proteger un derecho es evitar su vulneración.
- Ésta Dirección cumplió a cabalidad el procedimiento legal aplicable a este tipo de investigaciones, sujetándose estrictamente al procedimiento administrativo común, sin incurrir en la violación del derecho de defensa o contradicción de la recurrente: **comunicó el inicio de la investigación a Zoom; garantizó el derecho de la sociedad a ser oída, aportar y solicitar pruebas; y se garantizó el derecho de contradicción, con el análisis del recurso en cuestión**.
- Las ordenes que se le fueron impartidas a Zoom por la Superintendencia de Industria y Comercio son semejantes a aquellas que fueron acordadas con la Comisión Federal De Comercio De Los Estados Unidos De América.
- A pesar de que el campo de acción de Internet desborda las fronteras nacionales, para la Corte Constitucional el nuevo escenario tecnológico y las actividades en Internet no se sustraen del respeto de los mandatos constitucionales.
- **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, esta entidad ha sido respetuosa del principio de legalidad y ha obrado conforme con lo establecido en el derecho colombiano.

---

[53] 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/

[54] *Idem.*

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

[56] *Ibidem*.

SEXTO: Que, como consecuencia de la situación actual, y teniendo en cuenta el Estado de Emergencia Económica, Social y Ecológica decretado por el Gobierno Nacional, se ha restringido el ingreso a las instalaciones de la Superintendencia, en consecuencia, se establecieron las medidas pertinentes para permitir el acceso completo a los expedientes por medios digitales.

Al punto se precisa que, con el fin de garantizar los derechos fundamentales de la sociedad extranjera **ZOOM VIDEO COMMUNICATIONS, INC**, esta Dirección ha concedido el acceso al presente Expediente digital a esta, por intermedio de su apoderado vinculado al correo electrónico mjaramillo@gomezpinzon.com, quien debe registrarse en calidad de persona natural, exclusivamente con los datos en mención, en el enlace https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php.

En caso de que la sociedad requiera un acceso adicional de consulta del Expediente, deberá dirigir su solicitud en tal sentido desde el correo electrónico de notificación judicial de la sociedad, a los correos electrónicos contactenos@sic.gov.co y habeasdata@sic.gov.co, indicando los nombres y números de identificación de las personas autorizadas, acreditando para dicho efecto los debidos poderes y/o autorizaciones, según corresponda.

Finalmente, indicando que la totalidad del Expediente se encuentra digitalizado para su consulta por medios virtuales, si la sociedad **ZOOM VIDEO COMMUNICATIONS, INC** considera estrictamente necesario el acceso del Expediente en físico, deberá enviar un correo electrónico a contactenos@sic.gov.co y habeasdata@sic.gov.co, solicitando la asignación de una cita para revisión física del Expediente en las instalaciones de la Superintendencia de Industria y Comercio en la ciudad de Bogotá D.C., indicando el número de radicado. Lo anterior por cuanto se deben garantizar el ingreso a las instalaciones con las adecuadas medidas de bioseguridad.

SÉPTIMO: Se reitera que **una orden administrativa no es una sanción, sino una medida necesaria para la adecuación de las actividades u operaciones de los Responsables del Tratamiento a las disposiciones de la regulación colombiana sobre protección de datos personales.** Las sanciones por infringir la Ley Estatutaria 1581 de 2012 *-multas, suspensión de actividades, cierre temporal o definitivo-* están previstas en el artículo 23 de dicha norma. Allí se puede constatar que las órdenes no son sanciones.

OCTAVO: Que, analizadas todas las cuestiones planteadas, se encuentra que no fueron desvirtuados los argumentos que fundamentaron la resolución impugnada y teniendo en cuenta lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho confirmará la decisión contenida en la Resolución No. 74519 del 23 de noviembre de 2020.

En mérito de lo expuesto, este Despacho

RESUELVE

ARTÍCULO PRIMERO. Confirmar en todas sus partes la Resolución No. 74519 del 23 de noviembre de 2020 por las razones expuestas en la parte motiva de este acto administrativo.

ARTÍCULO SEGUNDO. Conceder el recurso subsidiario de apelación interpuesto en contra de la Resolución No. 74519 del 23 de noviembre de 2020, y en consecuencia dar traslado del presente expediente al despacho del Superintendente Delegado para la Protección de Datos Personales para que proceda de acuerdo con su competencia.

ARTÍCULO TERCERO. Notificar personalmente el contenido de la presente resolución a la sociedad extranjera ZOOM VIDEO COMMUNICATIONS, INC, a través de su apoderado o quien haga sus veces.

COMUÍQUESE, NOTIFÍQUESE Y CÚMPLASE
Dada en Bogotá, D.C., 25 AGOSTO 2021

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUÑOZ

ALC/CEZ

NOTIFICACIÓN:

Sociedad (1):	**ZOOM VIDEO COMMUNICATIONS, INC**
Identificación:	SIN IDENTIFICACIÓN[57]
Correo electrónico:	legal@zoom.us Nate.cooper@zoom.us
Dirección:	N/A
Ciudad:	San José (California)
Director de Privacidad:	Lynn Haaland
Apoderado:	Mauricio Jaramillo Campuzano
Identificación:	80.421.942
Tarjeta profesional:	No. 74.555 del C.S. de la J.
Correo:	mjaramillo@gomezpinzon.com
Dirección:	Calle 67 No. 7 – 35 Oficina 1204 Bogotá D.C.
Ciudad:	Bogotá D.C.

[57] No se cuenta con identificación