REPUBLICA DE COLOMBIA

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

RESOLUCIÓN NÚMERO 4551 DE 2022

(08 FEBRERO DE 2022)

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

Radicación Nº 21-11032

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, *modificado por el artículo 7 del Decreto 092 de 2022, y*

CONSIDERANDO

PRIMERO. Que mediante **Resolución Nº 29826 del 19 de mayo del 2021** 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 **WhatsApp LLC**.

Las ordenes administrativas de carácter preventivo que impartió esta autoridad mediante **Resolución Nº 29826 del 19 de mayo del 2021** fueron las siguiente:

> ***"PRIMERO. ORDENAR*** *a la sociedad WhatsApp LLC (en adelante* ***WhatsApp****) que respecto de los Datos personales que recolectan o tratan en el territorio de la República de Colombia sobre personas residentes o domiciliadas en este país, implementen un mecanismo o procedimiento apropiado, efectivo y demostrable para que, al momento de solicitar la Autorización al Titular, le informen en idioma castellano, de manera clara, sencilla y expresa todo lo que ordena el artículo 12 de la Ley Estatutaria 1581 de 2012, a saber:*
>
> *"a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;*
>
> *"b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;*
>
> *"c) Los derechos que le asisten como Titular;*
>
> *"d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento."*
>
> ***WhatsApp*** *como Responsable del Tratamiento, también deberá cumplir lo que ordena el parágrafo del citado artículo 12:*
>
> *"El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta."*
>
> ***PARÁGRAFO. WhatsApp*** *deberá cumplir lo anterior dentro del mes siguiente a la ejecutoria del presente acto administrativo. Asimismo, tendrá que remitir a la Dirección de Investigación de Protección de Datos Personales de esta entidad la evidencia del cumplimiento de lo ordenado en este artículo dentro de los cinco (5) días siguientes al vencimiento de dicho término.*
>
> ***ARTÍCULO SEGUNDO: ORDENAR*** *a WhatsApp LLC (en adelante* ***WhatsApp****) crear una Política de Tratamiento de Información (PTI) redactada en idioma castellano y que cumpla todos los requisitos que*

exige el artículo 13 del Decreto 1377 de 2013 (incorporado en el artículo 2.2.2.25.3.1 del Decreto 1074 de 2015). Dicha PTI debe ser puesta en conocimiento de los Titulares de los Datos domiciliados o residentes en el territorio colombiano.

***PARÁGRAFO. WhatsApp** deberá cumplir lo anterior dentro del mes siguiente a la ejecutoria del presente acto administrativo. Asimismo, tendrá que remitir a la Dirección de Investigación de Protección de Datos Personales de esta entidad la evidencia del cumplimiento de lo ordenado en este artículo dentro de los cinco (5) días siguientes al vencimiento de dicho término.*

***ARTÍCULO TERCERO: ORDENAR** a WhatsApp LLC (en adelante **WhatsApp**) que respecto de los Datos que recolectan o tratan en el territorio de la República de Colombia sobre personas residentes o domiciliadas en este país, registren sus Bases de Datos en el Registro Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio.*

***PARÁGRAFO. WhatsApp** deberá cumplir lo anterior dentro de los dos (2) meses siguientes a la ejecutoria del presente acto administrativo".*

SEGUNDO. Que mediante correo electrónico con radicado 21-11032- -00011 del 3 de agosto de 2021, la sociedad extranjera presentó escrito con el cual interpuso recurso de reposición y en subsidio de apelación contra la **Resolución Nº 29826 del 19 de mayo del 2021**. En el escrito la sociedad solicita que esta autoridad revoque la **Resolución Nº 29826 del 19 de mayo del 2021 "***y se abstenga de emitir y ejecutar órdenes contra la WhatsApp en relación con el supuesto tratamiento de datos personales en Colombia*". Lo anterior, con fundamento en:

A. <u>La SIC carece de jurisdicción y competencia para emitir la Resolución en contra de la Compañía</u>

En la toma de decisiones y en el ejercicio de su facultades de investigación y sanción la SIC debe ejercer sus poderes dentro de estrictos parámetros de legalidad. Este requisito garantiza que las decisiones de las entidades públicas sean coherentes con los poderes legales que les han sido delegados. En el contexto de las acciones y poderes limitados de una agencia administrativa, el concepto de "motivación" es primordial. Esto requiere que haya un vínculo causal entre los hechos en cuestión y la acción de una autoridad para hacer cumplir la ley. El Consejo de Estado ha explicado que la formulación de una investigación y de cargos (en este caso, de una orden final) no basta por sí sola para cumplir el requisito de la debida motivación.[1] Específicamente, una autoridad debe suministrar "fundamentos suficientes" para sus acciones haciendo referencia a argumentos específicos y explicaciones claras que determinen la motivación de la autoridad.
En este caso, la Resolución pretende regular el Servicio de WhatsApp bajo las disposiciones de la Ley de Protección de Datos Personales, la cual se aplica al tratamiento dentro de Colombia y que, como se explica más adelante, no tiene alcance extraterritorial. La Resolución carece de soporte probatorio para demostrar que el tratamiento que realiza WhatsApp se produce dentro del territorio colombiano, lo que constituye un defecto de fondo. Como toda orden que no esté debidamente respaldada por una disposición legal, la Resolución viola el principio de legalidad y debe ser revocada.

El ámbito de aplicación territorial de la Ley de Protección de Datos es claro. El artículo 2 de la Ley de Protección de Datos establece:

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

*El "tratamiento de datos personales" es definido como "[c]ualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión" (véase el Artículo 3 literal (g) de la Ley de Protección de Datos). Así, de acuerdo con su literalidad, la Ley de Protección de Datos aplica **únicamente**: (i) a entidades que traten datos personales dentro del territorio colombiano;[2] <u>o</u> (ii) a aquellas entidades no establecidas en Colombia que, bajo normas y tratados internacionales, están obligadas a cumplir con la normativa colombiana. La sentencia C-748 de 2011,*

---

[1] *Véase*, *Consejo de Estado, Sala de lo Contencioso Administrativo, Sección Tercera, sentencia del 9 de octubre de 2003, CP Germán Rodríguez Villamizar*. El más alto Tribunal administrativo ha explicado en múltiples sentencias que cuando una autoridad apoya sus actos o decisiones en hechos falsos o erróneos existe un vicio resultante en el acto administrativo que debe, a su vez, dar lugar a la anulación del propio acto.
[2] Artículo 2 de la Ley 1581 de 2012.

citada en la Resolución, apoya esta interpretación. Dicha sentencia deja claro que la Ley de Protección de Datos sólo se aplicará cuando se cumpla alguna de las dos circunstancias anteriores. Cualquier aplicación

que no se base en ninguno de los dos hechos descritos carecería de sustento legal y violaría el principio de legalidad.

De hecho, en consonancia con la teoría constitucional, la soberanía nacional sólo puede ejercerse dentro del territorio nacional de un Estado, ya que ejercer la autoridad fuera de dicho territorio implica intrínsecamente pasar por encima de la soberanía de otros países. La Corte Constitucional ha defendido en repetidas ocasiones el principio de territorialidad al considerar que:

> *"(…) tal y como lo precisó la Corte Internacional de Justicia en el caso del Estrecho de Corfú, este principio confiere derechos a los Estados, pero también les impone claras y precisas obligaciones internacionales, entre las cuales sobresale la de respetar la soberanía de las demás Naciones, en toda su dimensión".*[3]

Asimismo, la Corte Constitucional ha resaltado que :

> *"El principio de la territorialidad de la ley es consustancial con la soberanía que ejercen los Estados dentro de su territorio; de este modo cada Estado puede expedir normas y hacerlas aplicar dentro de los confines de su territorio"* [4]

Los expertos en la materia también están de acuerdo también con el alcance de este principio. [5]
De acuerdo con el principio de territorialidad, las autoridades colombianas sólo pueden hacer cumplir la ley colombiana estrictamente dentro del territorio colombiano con algunas excepciones explícitas[6]*, ninguna de los cuales aplica a este caso.*

De hecho, el legislador colombiano, siendo muy consciente de las limitaciones impuestas por el principio de territorialidad, limitó expresamente el ámbito de aplicación territorial de la Ley de Protección de Datos al redactar el artículo 2.

En el presente caso, la Resolución no incluye pruebas de ninguno de los dos supuestos de aplicación de la Ley de Protección de Datos. Por lo tanto, dicha ley no debe aplicarse a una empresa extranjera respecto de la cual la SIC no ha demostrado que trata datos personales en Colombia, y en consecuencia, la SIC carece de competencia y jurisdicción para emitir la Resolución.
La Resolución ni siquiera intenta aplicar la Ley de Protección de Datos "en virtud de normas y tratados internacionales ". Tampoco podría hacerlo. La Resolución no identifica qué norma o tratado internacional otorgaría jurisdicción a la autoridad colombiana sobre WhatsApp, una compañía extranjera que no trata datos personales en Colombia, pero tampoco explica cómo su interpretación sería compatible con disposición de ley o tratado alguno.

Por el contrario, el único fundamento por el que, según la Resolución, la Ley de Protección de Datos se aplica a WhatsApp es que la Compañía (supuestamente) trata datos personales en el territorio colombiano. A pesar de reconocer que ***WhatsApp no tiene presencia física en Colombia, la Resolución se basa en supuestos, respecto de los cuales no existe evidencia en el expediente, en relación con que WhatsApp instala cookies en Colombia y recopila datos dentro del territorio colombiano.***

*En particular, la Resolución (con breve argumentación) concluyó que, "**sin lugar a duda,** una cookie es un mecanismo que la investigada instala en los equipos o dispositivos (bien sea celular, computador portátil, u otro) de las personas residentes o domiciliadas en la República de Colombia con el objetivo de recolectar algunos de sus Datos Personales. Por tanto, WhatsApp realiza un Tratamiento de Datos Personales en el territorio colombiano sujeto a las disposiciones de la Ley 1581 de 2012". (énfasis añadido). Basándose en*

[3] Corte Constitucional. Sentencia C-1189 de 2000.

[4] Corte Constitucional. Sentencia T-1157 de 2000.

[5] H. Kelsen : *Teoría pura del derecho*. Editorial Universitaria de Buenos Aires. 1979 (16 edición), p. 195. Citado en Curso de Derecho Internacional. Yannick Galland, José Antonio Rivas. Pág. 123.

[6] Corte Constitucional. Sentencia T-1157 de 2000.

lo anterior, la Resolución determinó (incorrectamente) que había competencia de acuerdo con el artículo 2 de la Ley de Protección de Datos.

De acuerdo con los claros términos del referido artículo 2 y los principios de soberanía internacional, instamos respetuosamente a la SIC a que revoque la Resolución, ya que extiende la autoridad de la SIC bajo la Ley de Protección de Datos para alcanzar cualquier sitio web al que se acceda desde Colombia y que utilice cookies. Como se describe más adelante, dada la omnipresencia del uso de cookies en todo el

mundo, esto efectivamente otorga a la SIC jurisdicción global e ilimitada, violando tanto los términos de la Ley Protección de Datos como la soberanía de otras naciones.

i. *El solo uso de cookies no implica el tratamiento de datos personales en Colombia ni el uso de ningún servidor u otra infraestructura (es decir, medios) ubicados en Colombia.*

Es importante aclarar que 1) las cookies tienen un rol muy limitado en la operación del servicio de WhatsApp[7], especialmente cuando se trata de la aplicación de WhatsApp en dispositivos móviles, y 2) el solo uso de cookies no conlleva actividades de tratamiento de datos personales en Colombia.
Las conclusiones de la Resolución sobre el supuesto uso de cookies por parte de WhatsApp no incluyen pruebas que expliquen cómo funcionan las cookies de WhatsApp ni el tratamiento de datos personales que realiza.

Como punto de partida, WhatsApp rechaza la premisa de que sus actividades de tratamiento de datos personales (a través de cookies o de otro cualquier otro modo) se realicen en Colombia y que utilice medios situados en el territorio colombiano para el tratamiento de datos personales. Todos los actos de tratamiento de datos personales se realizan en los servidores de WhatsApp, los cuales están ubicados fuera del territorio colombiano, por lo que, de conformidad con el artículo 2 de la Ley de Protección de Datos, no hay jurisdicción sobre dichas actividades de tratamiento.

El hecho de que WhatsApp pueda utilizar cookies para el funcionamiento de la versión web de su aplicación (la cual, como se explicó anteriormente es una función complementaria y no es necesaria para operar el servicio) o del sitio web de WhatsApp no cambia la premisa fundamental de que el tratamiento de datos personales subyacente para prestar el servicio de WhatsApp, incluido el relacionado con cualquier dato asociado a una cookie, se realiza fuera del territorio colombiano.

Las cookies son omnipresentes en Internet y sirven para una variedad de funciones (en su mayoría útiles), tales como mostrar al usuario el contenido en el lenguaje de su preferencia. Como explica WhatsApp en su sitio web público, una cookie es "un archivo de texto que se almacena en tu computadora o teléfono móvil cuando visitas una página web"[8] Por lo tanto, las cookies no son servidores, cables o cualquier otra operación técnica u organizacional para realizar el tratamiento de datos, son simplemente un archivo de datos en sí mismo, que permite a un proveedor de servicios reconocer o identificar a un navegador. Cada vez que un usuario accede a un sitio web a través de un navegador, el usuario está esencialmente solicitando al navegador que acceda a un servidor y que extraiga algún contenido ubicado allí, para que pueda ser mostrado al usuario. La primera vez que un usuario visita ese sitio web, no hay cookies previas involucradas. Sin embargo, el comportamiento predeterminado de un navegador es mostrar al usuario el contenido del sitio web solicitado y, mientras envía las cookies asociadas de ese sitio web, las guarda en el dispositivo del usuario, como un archivo en el historial de navegación. Estas cookies luego se envían de vuelta al servidor que las originó, en cualquier solicitud posterior para llegar nuevamente al mismo sitio web, donde se almacenan y tratan. Cualquier actividad de tratamiento de datos personales ocurre en el servidor del sitio web.

Contrario a lo establecido en la Resolución, la sola colocación de una cookie en un navegador no se encuentra dentro del alcance de la Ley de Protección de Datos. Esto se debe a que la colocación de una cookie en un navegador no implica ni la recolección ni cualquier otro tipo de tratamiento de datos personales en Colombia, ni el uso de ningún servidor ni de otra infraestructura (es decir, un medio) ubicado en Colombia.

[7] Ver: www.whatsapp.com/legal/cookies?lang=es Visitado el 2 de agosto de 2021.
[8] Ibídem.

Como ocurre con cualquier dato que se entrega a WhatsApp, es el usuario quien "va" al exterior a través de las redes para acceder a los servidores de la Compañía en el exterior. Dicho de otra manera, el usuario, cuando utiliza WhatsApp, utiliza activamente las redes de telecomunicaciones como medio para acceder a los servidores de WhatsApp (ubicados en el extranjero) y el servidor de WhatsApp mostrará el contenido solicitado al navegador (que se lo muestra al usuario), y con los archivos de cookies asociados

al mismo. En consecuencia, en todos los casos, cualquier tratamiento de datos personales se realiza en los servidores ubicados en el exterior y no en Colombia.

A modo de analogía, meramente explicativa, una cookie podría ser similar a una suscripción a una revista, donde el suscriptor en Colombia solicita una revista a un proveedor ubicado en el exterior. El suscriptor podrá seleccionar sus preferencias y las comunicará al proveedor que recibirá y almacenará la información en el exterior. El proveedor almacenará estos registros para personalizar la selección de la revista, mediante un código único de referencia, que es proporcionado al suscriptor. La revista y su contenido se producen fuera de Colombia. El código también se puede utilizar para realizar analítica para mejorar las revistas para todos los usuarios. Tal propósito es comunicado y autorizado por el usuario de WhatsApp. Dicho análisis se realiza fuera de Colombia.

Es importante destacar que el Servicio de WhatsApp opera completamente fuera de la jurisdicción, es decir, en servidores ubicados en el extranjero. No hay ninguna actividad en Colombia. Por lo tanto, incluso si las cookies en sí mismas fueran un medio para "tratar" datos personales (y no lo son; son simplemente un pequeño archivo de texto), dicho tratamiento se llevaría a cabo en los servidores de WhatsApp fuera de Colombia. En otras palabras, cualquier dato proporcionado por los usuarios ubicados en Colombia "viaja" a través de las redes y finalmente es tratado a través de servidores alojados en ubicaciones fuera de Colombia.

Con base en lo anterior, el principal argumento de la Resolución de que WhatsApp trata datos personales en Colombia es infundado y debe ser reconsiderado.

Además, WhatsApp solicita respetuosamente a la SIC que considere las implicaciones extremadamente amplias de su conclusión jurisdiccional errónea. Las cookies son tan intrínsecas al funcionamiento normal de Internet que la interpretación incluida en la Resolución implicaría que la legislación colombiana aplicaría efectivamente a cualquier sitio web del mundo al que simplemente acceda una persona en Colombia, sin importar si se trata de sitios web comerciales, civiles o gubernamentales.

Ese alcance es incompatible con el ámbito territorial pretendido por la Ley de Protección de Datos, y conduciría a una aplicación de la Ley de Protección de Datos que sobrepasa todos los límites territoriales y de soberanía. Si la ley pretendiera un alcance tan global, lo habría dicho claramente; en cambio, prevé un alcance más estrecho y matizado para el tratamiento de datos personales que verdaderamente se lleva a cabo dentro de Colombia. De hecho, esta interpretación haría que la segunda cláusula del artículo 2 fuera redundante porque nunca sería necesario basarse en tratados internacionales para aplicar la Ley de Protección de Datos a entidades extranjeras si el "tratamiento de datos" se interpretara de manera tan amplia. Claramente, la interpretación de la Resolución es irrazonable y defectuosa, y, respetuosamente, la SIC no tenía jurisdicción para emitir la Resolución.

(…)

ii. La Resolución incluye órdenes amplias que afectan mucho más que el supuesto tratamiento de datos relacionados con cookies de WhatsApp en Colombia.

La Resolución se basa en la supuesta jurisdicción de la SIC sobre WhatsApp debido a sus inexistentes actividades de tratamiento de datos relacionados con las cookies en territorio colombiano. Sin embargo, las órdenes incluidas en la Resolución, sin ninguna justificación, van mucho más allá del uso de cookies por parte de WhatsApp y, en última instancia, se refieren a datos que, como se explica en la Respuesta de WhatsApp, se tratan fuera de Colombia en los servidores de la Compañía.

De hecho, a pesar de que varias de las órdenes en la Resolución se limitan nominalmente a "los Datos personales que recolectan o tratan en el territorio de la República de Colombia", esta limitación no tiene implicación alguna en última instancia, ya que la Resolución requiere que WhatsApp realice cambios con respecto a la información que entrega y que se relaciona con todo tipo de tratamiento de datos (incluida la gran mayoría del tratamiento de datos de WhatsApp que no tiene nada que ver con las cookies).

Adicionalmente, la Resolución no identifica exactamente cómo interpretar "medios para el tratamiento" ni qué datos personales supuestamente recopila WhatsApp mediante cookies. Esta es una pieza central de información que se extraña en el análisis de la Resolución, y que hace que el reclamo jurisdiccional de la SIC sea infundado y, al mismo tiempo, hace que las órdenes allí contenidas sean excesivamente amplias e indebidas.

La SIC no debe utilizar las "cookies" como fundamento para asumir mayores poderes regulatorios que los que le otorga la Ley de Protección de Datos y extender su jurisdicción para llegar a todos los sitios web que utilizan cookies y todas las demás actividades de tratamiento de datos no relacionadas directamente con el uso de cookies, incluyendo los sitios web de entidades públicas y privadas de todo el mundo. Y, aunado a lo anterior, la SIC no debería utilizar esta malinterpretación jurisdiccional para tratar de ampliar aún más esos poderes al intentar regular las actividades de tratamiento de datos que no tienen conexión con las cookies y que ocurren fuera del territorio colombiano.

En vista de lo anterior, la Resolución debe ser revocada por falta de jurisdicción, ya que, respetuosamente, la SIC no sólo ignoró la manera en que funcionan las cookies y malinterpretó el artículo 2 de la Ley de Protección de Datos, sino que también emitió órdenes excesivas que van mucho más allá del uso de cookies por parte de WhatsApp.

Además, es necesario tener en cuenta que WhatsApp informa a los usuarios y obtiene su autorización antes de que éstos comiencen a utilizar los servicios, le informa sobre los términos de su Política de Tratamiento de Datos Personales, que sobre el particular señalan en la sección "Información que recopilamos" que WhatsApp utiliza "cookies para operar y proporcionar nuestros Servicios, además de proporcionarte nuestros Servicios basados en Internet, mejorar tus experiencias, entender cómo se usan nuestros Servicios y personalizarlos".

De acuerdo con la información proporcionada, los usuarios pueden comprender el propósito del tratamiento que realiza WhatsApp, que utilizará cookies y cómo pueden controlar las cookies e incluso deshabilitarlas, según sus preferencias, después de que decidan utilizar el servicio, o pueden decidir no utilizar la versión web complementaria y opcional. Por lo tanto, de acuerdo con el artículo 7 del Decreto 1377 de 2013, WhatsApp puede entender válidamente que mediante conductas inequívocas, los usuarios que reconocen las políticas de WhatsApp y continúan utilizando los servicios de la Compañía, otorgaron su autorización para que WhatsApp trate sus datos fuera del territorio colombiano. La SIC parece desconocer los efectos de dicha autorización informada a través de conductas inequívocas de los usuarios.

B. La Resolución violó los derechos al debido proceso de WhatsApp.

i. La Resolución se emitió en violación de los derechos de defensa y contradicción de WhatsApp

La Resolución le negó a WhatsApp la posibilidad de ejercer su derecho de defensa y de contradecir la conclusión de la Resolución según la cual WhatsApp trata datos personales dentro de Colombia (de la cual depende toda la validez de la Resolución). Sólo por esta razón, solicitamos respetuosamente que la SIC revoque la Resolución.

Las normas constitucionales y legales de Colombia requieren que las autoridades administrativas garanticen a los investigados el derecho de defensa y contradicción mediante procedimientos administrativos en los que las partes puedan defenderse y presentar pruebas. Por ejemplo, de acuerdo con el artículo 34 del CPACA, los procedimientos administrativos requieren que las partes interesadas tengan la oportunidad de controvertir la prueba y pronunciarse sobre las mismas. Haciendo eco de este principio, el Consejo de Estado ha establecido que:

"No sólo razones de justicia avalan la solución propuesta, sino la de garantizar adecuadamente el derecho de defensa en una actuación administrativa que puede conducir a una afectación grave del patrimonio económico de una persona y a sus derechos fundamentales, e igualmente, la necesidad de preservar los principios de igualdad, celeridad, economía, eficiencia y eficacia de las actuaciones administrativas, en el sentido de que en forma rápida y oportuna se defina si hay lugar o no a iniciar el respectivo juicio de responsabilidad fiscal, porque sin habérsele dado oportunidad al posible imputado de exponer su versión de los hechos y de producir la prueba de descargo, únicamente se cuenta con una verdad unilateral".

La Resolución simplemente concluye, sin haber abordado nunca el tema con WhatsApp, que la Compañía trata datos personales dentro de Colombia. Esta conclusión es la premisa de la que depende

completamente la Resolución, y WhatsApp nunca tuvo la oportunidad de impugnarla (lo pudo hacer en su respuesta al Requerimiento donde afirmó lo contrario como parte de su respuesta a otra pregunta que no guarda relación con la Resolución).

Los tribunales colombianos han sostenido que la participación del investigado en los procedimientos administrativos (ausente en esta ocasión) es legalmente requerida, ya que es la única forma de dar certeza a la acción de la autoridad y garantizar los derechos del sujeto investigado:

"La participación del presunto imputado en la etapa de investigación permite asegurar no sólo el derecho de defensa sino que contribuye a dar certeza a aquélla, y a garantizar su eficiencia y eficacia, porque es posible determinar en forma pronta y oportuna que no hay lugar a exigirle la responsabilidad fiscal a aquél, o que por el contrario, se requiere adelantar el trámite del juicio para establecer si hay lugar a declararla o no". (Énfasis propio)

En efecto, la Corte Constitucional ha establecido que el derecho a la defensa es una de las garantías mínimas requeridas antes de que una autoridad administrativa emita una orden como la Resolución:

"La jurisprudencia constitucional ha diferenciado entre las garantías previas y posteriores que implica el derecho al debido proceso en materia administrativa. Las garantías mínimas previas se relacionan con aquellas garantías mínimas que necesariamente deben cobijar la expedición y ejecución de cualquier acto o procedimiento administrativo, tales como el acceso libre y en condiciones de igualdad a la justicia, el juez natural, el derecho de defensa, la razonabilidad de los plazos y la imparcialidad, autonomía e independencia de los jueces, entre otras. De otro lado, las garantías mínimas posteriores se refieren a la posibilidad de cuestionar la validez jurídica de una decisión administrativa, mediante los recursos de la vía gubernativa y la jurisdicción contenciosa administrativa" (Énfasis propio)

Finalmente, la Corte Constitucional ha reconocido que el debido proceso garantiza que los investigados tengan derecho a contradecir las pruebas utilizadas en su contra. Para que este derecho tenga algún relevancia y aplicación, se requiere que las partes conozcan de antemano las pruebas y los cargos imputados, lo que aquí no ocurrió. De hecho, la SIC sólo emitió el Requerimiento, que contenía preguntas enfocadas en la Actualización; nunca hubo indicios de que la SIC estuviera interesada en demostrar que WhatsApp trataba datos en Colombia (especialmente porque la Compañía no tiene ni usa ninguna presencia local), y la SIC no incluyó preguntas en el Requerimiento sobre este punto.

Estos principios del debido proceso no solo sirven a los investigados: también garantizan que las decisiones administrativas se tomen después de un adelantar un análisis fáctico adecuado y se basen en conclusiones legales racionales. De esta forma, el derecho de defensa sustenta el principio de legalidad, ya que sólo después de un riguroso debate probatorio se puede dictar una orden administrativa válida.

En este sentido, la Corte Constitucional ha dictaminado que se viola el derecho de defensa si, como sucedió aquí con respecto a la conclusión de la Resolución de que WhatsApp trata datos personales en Colombia, no se permite que la persona afectada por una decisión administrativa sea escuchada o pueda contradecir las pruebas aducidas en su contra. En Sentencia T-1341 de 2001, la Corte Constitucional estableció que :

"i.) La efectividad de ese derecho en las instancias administrativas supone la posibilidad de que el administrado interesado en la decisión final que se adopte con respecto de sus derechos e intereses, pueda cuestionarla y presentar pruebas, así como controvertir las que se alleguen en su contra (CP, art. 29), pues, a juicio de la Corte, de esta forma se permite racionalizar el proceso de toma de decisiones administrativas, en tanto que "ello evidentemente constituye un límite para evitar la arbitrariedad del poder público" (Énfasis propio)

En este caso, WhatsApp nunca tuvo la oportunidad de controvertir la conclusión errónea de la Resolución de que trata datos en Colombia ni de presentar pruebas para refutarla (de hecho, la evidencia que sí proporcionó WhatsApp sobre este tema sugiere lo contrario).

En la única pregunta del Requerimiento de la SIC relacionada remotamente con la conclusión legal clave de la Resolución, se preguntó "¿En qué país o países se almacenarán los Datos de los usuarios residentes o domiciliados en la República de Colombia?". En respuesta, WhatsApp describió específicamente dónde podría ocurrir el almacenamiento de datos (y no mencionó a Colombia):

"WhatsApp puede recolectar, transferir, almacenar y procesar información del usuario hacia o en ubicaciones globales donde tiene o usa instalaciones, y donde se encuentran los proveedores de servicios de WhatsApp o los afiliados y socios de Facebook, independientemente de dónde los usuarios utilicen Servicios de WhatsApp".

De ninguna manera la respuesta de WhatsApp respalda la conclusión errónea de la Resolución de que trata datos personales en Colombia. Esto tiene sentido, porque WhatsApp de hecho no trata datos en Colombia; por ejemplo, no tiene ni utiliza ninguna instalación allí.

Adicionalmente, la respuesta de WhatsApp señaló específicamente que "WhatsApp presenta esta respuesta de forma voluntaria. Sin embargo, la presentación de esta respuesta no debe ser interpretada más allá de la intención de WhatsApp de cooperar con la SIC y, por lo tanto, no debe ser interpretada como un reconocimiento por parte de WhatsApp de la jurisdicción de la SIC". De esta forma, la SIC tuvo conocimiento de que su conclusión errónea sobre jurisdicción sería controvertida por WhatsApp. Pero en lugar de permitirle cualquier oportunidad, entre otras cosas, para explicar por qué la teoría infundada de la SIC malinterpreta la naturaleza de las cookies y por qué WhatsApp no procesa datos en Colombia, la autoridad simplemente emitió la Resolución.

Como resultado, WhatsApp no tuvo la oportunidad (garantizada por la ley colombiana) de presentar sus contraargumentos, disputar los hechos y (falta de) pruebas en los que se basan las conclusiones erróneas de la Resolución, o presentar sus conclusiones sobre este punto jurisdiccional clave. antes de que la SIC adoptara la Resolución.

Esta falta de debido proceso también viola la ley de Protección de Datos, que establece que la SIC solo puede emitir órdenes si, como resultado de una investigación, concluye que son necesarias para proteger los derechos de protección de datos de los titulares en Colombia. Sin embargo, la SIC no abrió una investigación en la que WhatsApp tuviera la oportunidad de presentar una defensa. la Compañía ni siquiera recibió aviso sobre la existencia de una investigación formal en su contra. Por lo tanto, más allá de violar los derechos al debido proceso de WhatsApp bajo la ley colombiana, la Resolución violó la propia Ley de Protección de Datos.

El solo hecho de que la SIC formuló el Requerimiento no justifica la Resolución, sobre todo porque el Requerimiento ignoró el tema que subyace la base de toda la Resolución: el (infundado) supuesto de que WhatsApp trata datos personales en Colombia. Especialmente dado que no tiene ni utiliza instalaciones en Colombia, WhatsApp nunca fue notificado (ni siquiera de manera implícita) de que la SIC buscaba probar esta afirmación.

(…)

ii. La Resolución desconoció la presunción de inocencia de WhatsApp.

Por similares razones, la Resolución desconoce la presunción de inocencia de WhatsApp contenida en el artículo 29 de la Constitución Política, según la cual "[…] Toda persona se presume inocente mientras no se la haya declarado judicialmente culpable. Quien sea sindicado tiene derecho a la defensa y a la asistencia de un abogado escogido por él, o de oficio, durante la investigación y el juzgamiento […]". Lo anterior, al concluir simplemente que WhatsApp trató datos personales en Colombia sin permitirle montar una defensa, presumió que WhatsApp era "culpable", por presuntamente no cumplir con una normativa que no le era de aplicación.

En reiterada jurisprudencia, la Corte Constitucional ha señalado que el principio de presunción de inocencia es aplicable como criterio general en el derecho administrativo. En este sentido afirmó que:

"[…] La presunción de inocencia sólo puede ser desvirtuada mediante una mínima y suficiente actividad probatoria por parte de las autoridades represivas del Estado. Este derecho fundamental se profana si a la persona se le impone una sanción sin otorgársele la oportunidad para ser oída y ejercer plenamente su defensa" .

En este caso, la Resolución se emitió sin brindarle a WhatsApp la capacidad de defender, contradecir o presentar evidencia sobre la conclusión clave de la Resolución de que trató datos personales en

Colombia. La Resolución simplemente concluyó (erróneamente) sin investigar completamente el uso de cookies de WhatsApp o escuchar el argumento de WhatsApp.

A WhatsApp no se le concedió el beneficio de la duda sobre este punto crucial de la Resolución, y la Resolución también debe ser revocada por violar el artículo 29 de la presunción de inocencia de la Constitución Política.

iii. La Resolución se emitió sin tener en cuenta el principio de publicidad, dañando el buen nombre y la reputación de WhatsApp.

Finalmente, WhatsApp respetuosamente señala que la Resolución no fue debidamente notificada, lo que violó el derecho al debido proceso de WhatsApp bajo el principio de publicidad en los procesos administrativos.

La Corte Constitucional se ha referido al principio de publicidad como parte del debido proceso, señalando que :

"Los actos administrativos, por disposición del legislador, admiten dos formas concretas de publicidad, su publicación en el diario oficial, gaceta o cualquier otro medio oficial de divulgación, si se trata de contenidos abstractos u objetivos, esto es impersonales, y la notificación, si se trata de contenidos subjetivos y concretos que afectan a un individuo en particular, o a varios, identificables y determinables como tales, lo anterior por cuanto la publicidad se ha establecido como una garantía jurídica con la cual se pretende proteger a los administrados, brindándoles a éstos certeza y seguridad en las relaciones jurídicas que emanan de su expedición. En cuanto a los actos administrativos subjetivos, cuya acción de nulidad tenga caducidad, ellos deberán ser debidamente publicitados" (Énfasis propio)

En particular, la indebida notificación de un fallo administrativo constituye per se una violación del debido proceso e implica que el procedimiento administrativo que dio lugar al fallo careció de las debidas garantías. El resultado de tal incumplimiento es que la sentencia no es ejecutable. De manera similar, el artículo 72 del CPACA establece que, cuando una autoridad notifique indebidamente una decisión, la decisión no tendrá ningún efecto legal.

Aquí, la SIC publicó la Resolución en internet, poniéndola automáticamente a disposición de los medios de comunicación, y publicó la información en las redes sociales antes de notificar a WhatsApp el acto administrativo en su contra. Debido a que la Resolución es de naturaleza específica y está dirigida a una parte específica, debería haberse notificado primero en WhatsApp. El error no es meramente formal, la decisión de la SIC de publicar la Resolución mediante un comunicado de prensa antes de notificar a WhatsApp dañó el buen nombre y la reputación de WhatsApp en Colombia (sugiriendo erróneamente a los 39 millones de usuarios de WhatsApp que la Compañía infringió la Ley de Protección de Datos, lo que simplemente no es cierto).

Al concluir arbitraria y erróneamente (sin permitir que WhatsApp interviniera o se defendiera) que: (a) la Ley de Protección de Datos se aplica a WhatsApp; y así (b) WhatsApp violó la Ley de Protección de Datos, la SIC ha caracterizado innecesariamente a WhatsApp como un infractor de la ley a los ojos de su base de consumidores de Colombia.

El derecho al buen nombre y la reputación está reconocido en varios instrumentos de derecho internacional, como el artículo 12 de la Declaración Universal de Derechos Humanos ("Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación"), y el artículo 11 de la Convención Americana sobre Derechos Humanos ("Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad").

El artículo 15 de la Constitución Política establece que "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre" (Énfasis propio).

Como se señala en la jurisprudencia de la Corte Constitucional :

"Se tiene entonces que la intimidad, el buen nombre y la honra, son derechos constitucionalmente garantizados, de carácter fundamental, lo cual comporta, no sólo que para su protección se puede actuar directamente con base en la Constitución cuando a ello haya lugar, a través de la acción de tutela, sino

que, además, de las propias normas constitucionales, se desprende la obligación para las autoridades de proveer a su protección frente a los atentados arbitrarios de que sean objeto" (Énfasis propio).

En el caso de las personas jurídicas, como WhatsApp, la Corte Constitucional ha determinado que "El núcleo esencial de este derecho, consagrado en el artículo 15 de la Constitución, permite proteger a las personas jurídicas ante la difamación que le produzcan expresiones ofensivas o injuriosas. "Es la protección del denominado good will en el derecho anglosajón, que es el derecho al buen nombre de una persona jurídica y que puede ser estimado pecuniariamente" .

Con respecto a las personas jurídicas, la Sala Plena del Consejo de Estado definió "buen nombre" o "good will " de la siguiente manera :

"(…) al prestigio, que tiene un establecimiento mercantil, o un comerciante, frente a los demás y al público en general, es decir, al factor específico de un negocio que ha forjado fama, clientela y hasta una red de relaciones corresponsales de toda clase, aunado a la confianza que despierta entre los abastecedores, empleados, entidades financieras y, en general, frente al conjunto de personas con las que se relaciona (…) " (Énfasis propio).

Asimismo, el Consejo de Estado ha sostenido que, entre otros, los siguientes aspectos comprenden la noción de " good will " antes mencionada:

"además de la proyección de los beneficios futuros, la existencia de bienes incorporales, tales como la propiedad industrial, fórmulas químicas, procesos técnicos; la excelente ubicación en el mercado, la experiencia, la buena localización, la calidad de la mercancía o del servicio, el trato dispensado a los clientes, las buenas relaciones con los trabajadores, la estabilidad laboral de los mismos, la confianza que debido a un buen desempeño gerencial se logre crear en el sector financiero…" (Énfasis propio).

En este caso, sin notificarle la Resolución a WhatsApp , la SIC publicó un comunicado de prensa lo que llevó a muchos periódicos y medios de comunicación nacionales a replicar la conclusión errónea de que WhatsApp violó la Ley de Protección de Datos, afectando la reputación de WhatsApp. Algunas de las noticias incluían los siguientes titulares "Política de WhatsApp incumple la mitad de los requisitos que exige Colombia: SIC" , "La SIC ordenó a WhatsApp cumplir con normas de tratamiento de datos personales en Colombia" , "Ordenan a WhatsApp cumplir estándar nacional de protección de datos en Colombia" , "Superindustria ordenó a WhatsApp cumplir con las disposiciones legales de habeas data" . Todos estos informes de noticias se basaron completamente en la Resolución e identifican a WhatsApp como un completo infractor de la Ley de Protección de Datos, lo cual, como se estableció anteriormente, ni siquiera se aplica aquí para empezar.

En conclusión, la violación por parte de la SIC del principio de publicidad (al notificar indebidamente a WhatsApp de la Resolución) dañó severamente el buen nombre y reputación de WhatsApp en Colombia y otros lugares. Esto es especialmente grave considerando la invalidez procesal y sustantiva del hallazgo de la Resolución de que la Ley de Protección de Datos se aplica a WhatsApp (discutido anteriormente en Secciones III.A y III.B). Como ya se argumentó extensamente, WhatsApp no está obligado a cumplir con la Ley de Protección de Datos porque no trata datos personales en Colombia.

La Resolución impactó el buen nombre, reputación y posición de WhatsApp, lo que ha interferido con su capacidad para cumplir con su objeto social. Como resultado de la conclusión de la Resolución de que WhatsApp trató datos personales en Colombia, WhatsApp ha sido condenado ante el público en general y sus usuarios como una supuesta entidad infractora de la ley. Esto es particularmente perturbador para WhatsApp, cuyo modelo de negocio se basa en la confianza de sus usuarios (por lo que asegura la protección de los datos de sus usuarios mediante el cifrado de extremo a extremo).

(…)

C. La Resolución carece de fundamento legal y probatorio.

i. La conclusión de la Resolución de que WhatsApp trata datos personales en Colombia no tiene sustento probatorio y es contraria a la prueba en el expediente.

La Resolución debe ser revocada porque fue emitida: (i) con base en hechos no probados; (ii) hechos que fueron ignorados; o (iii) fue contraria a hechos probados. Como resultado, la SIC emitió la Resolución sin fundamento legal, ya que la Ley de Protección de Datos claramente no era aplicable.

La conclusión de la Resolución de que WhatsApp trató datos en Colombia, más allá de basarse en procedimientos erróneos, fue contraria a la evidencia en el expediente. Debido a que depende totalmente de esta conclusión, la falta de material probatorio sobre la misma, por defecto, significa que la Resolución se basa en declaraciones erróneas y está falsamente motivada, por lo que la SIC debe revocar la Resolución.

En particular, la conclusión errónea de la Resolución violó el artículo 42 del CPACA y el artículo 164 del Código General del Proceso de Colombia (en adelante, "CGP"). El artículo 42 del CPACA establece que :

"Habiéndose dado oportunidad a los interesados para expresar sus opiniones, y con base en las pruebas e informes disponibles, se tomará la decisión, que será motivada." (Énfasis propio).

Asimismo, el artículo 164 del CGP, aplicable en virtud de los artículos 211 y 306 del CPACA, establece:

"Toda decisión judicial debe fundarse en las pruebas regular y oportunamente allegadas al proceso. Las pruebas obtenidas con violación del debido proceso son nulas de pleno derecho".

Dada la importancia de la prueba, la Corte Constitucional sostuvo que :

"Esas garantías se encuentran relacionadas entre sí, de manera que -a modo de ejemplo- el principio de publicidad y la notificación de las actuaciones constituyen condición para el ejercicio del derecho de defensa, y la posibilidad de aportar y controvertir las pruebas, una herramienta indispensable para que las decisiones administrativas y judiciales se adopten sobre premisas fácticas plausibles. De esa forma se satisface también el principio de legalidad, pues solo a partir de una vigorosa discusión probatoria puede establecerse si en cada caso se configuran los supuestos de hecho previstos en las reglas legislativas y qué consecuencias jurídicas prevé el derecho para esas hipótesis" (Énfasis propio).

En este caso, la Resolución concluye que la SIC tiene jurisdicción sobre WhatsApp con base en hechos sobre la naturaleza y ubicación del uso de cookies por parte de la Compañía, que no fueron probados en el curso de un procedimiento administrativo. Como se describió anteriormente, este tema no fue abordado por el Requerimiento. Dado que la SIC, respetuosamente, no realizó una investigación exhaustiva para recopilar las pruebas necesarias para comprender los hechos, la conclusión no tuvo sustento.

Igualmente, la SIC ignoró la evidencia que sí tenía sobre este tema (proporcionada por WhatsApp como respuesta al Requerimiento). En su respuesta, WhatsApp no declaró específicamente que trató datos en Colombia y, de hecho, puso de presente que trató datos en otros lugares (que es, de hecho, el caso). Estos elementos del expediente, que socavan por completo la base jurisdiccional de toda la Resolución, contradicen la conclusión final (errónea) de que WhatsApp trata datos personales en Colombia.

Debido a la falta de evidencia de que WhatsApp trató datos personales en Colombia, la Resolución fue emitida erróneamente bajo la Ley de Protección de Datos, que claramente no es aplicable a WhatsApp y, como resultado, la Resolución también carece de fundamento legal.

En resumen, las conclusiones de la Resolución con respecto a la ubicación y la naturaleza del tratamiento de datos de WhatsApp no estaban respaldadas y eran contrarias a la evidencia en el expediente. Además, tales conclusiones no eran meros puntos complementarios: como hallazgos jurisdiccionales, determinan la validez de toda la Resolución. WhatsApp respetuosamente insta a la SIC a revocar la Resolución, que carecía de sustento fáctico y legal.

ii. La Resolución se basa en una interpretación errónea del marco legal de Protección de Datos de Colombia y concluye incorrectamente que WhatsApp no cumple con los requisitos de la Ley de Protección de Datos.

La Resolución concluye que WhatsApp no cumple con los requisitos de la Ley de Protección de Datos (que en cualquier caso no se aplica a las prácticas de datos de WhatsApp, como se detalla anteriormente). Por el contrario, a pesar de no estar obligado a cumplir con la ley colombiana, De hecho, la Política de Tratamiento de Datos Personales de WhatsApp de hecho incluye los requisitos mencionados en la orden y ha adoptado medidas de cumplimiento de la privacidad a nivel mundial.

(…) la Política de Tratamiento de Datos Personales de WhatsApp ya incluye garantías y protecciones a los usuarios que son compatibles con las órdenes emitidas por la Resolución y, además, los artículos del Centro de Ayuda contribuyen a brindar una transparencia adicional. Considerando las representaciones previas de la propia SIC en otros asuntos relacionados con casos similares , donde ha determinado que

los responsables del tratamiento, no la SIC, son los que tienen la capacidad de determinar los medios más efectivos para garantizar los derechos de los titulares, que es lo que sucedió en este caso, las órdenes son redundantes y respetuosamente deben ser revocadas.

Finalmente, es importante reiterar que los mensajes enviados a través del Servicio de WhatsApp (incluyendo mensajes de negocios)están cifrados de extremo a extremo y no pueden ser leídos por WhatsApp. Con el cifrado de extremo a extremo, los mensajes de los usuarios están protegidos con un candado, y sólo el destinatario y el remitente tienen la llave especial necesaria para desbloquearlos y leerlos. Este proceso se realiza automáticamente. El protocolo de cifrado de extremo a extremo de

WhatsApp está diseñado para prevenir a terceros y a WhatsApp de tener acceso a los mensajes o llamadas.

(…)

D. La Resolución fue emitida violando el principio de buena fe establecido por la Constitución colombiana al violar la confianza legítima de WhatsApp.

Como se especificó anteriormente y en su respuesta al Requerimiento de la SIC, WhatsApp no reconoce que esté dentro de la aplicación de la Ley de Protección de Datos, o que violó la Ley de Protección de Datos. Pero incluso si la SIC (erróneamente) concluye lo contrario, WhatsApp respetuosamente insta a la SIC a revocar la Resolución con base en el principio de buena fe de la Constitución de Colombia. Al decidir repentinamente aplicar la Ley Protección de Datos a WhatsApp respecto de presuntas infracciones (que WhatsApp sigue impugnando), pero que en cualquier caso habrían estado a la vista pública durante años, la SIC violó la confianza legítima de WhatsApp y, por lo tanto, violando el principio constitucional del bien fe vinculante a las autoridades públicas. Por tal motivo, WhatsApp insta a la SIC a revocar la Resolución.

La Constitución colombiana eleva el principio de buena fe a un estándar constitucional que rige la conducta tanto de los poderes públicos como de los privados, y juega un papel de suma importancia en el ordenamiento jurídico colombiano.

Como extensión del principio de buena fe, la Corte Constitucional ha reconocido la aplicabilidad de un concepto bien desarrollado en el derecho internacional, que es, la confianza legítima entre las partes. Este es un concepto de gran relevancia para las relaciones entre autoridades públicas y sujetos regulados. En particular, este concepto se ha convertido en un claro límite frente a los actos arbitrarios o abusivos realizados por autoridades públicas.

En palabras de la Corte Constitucional, la confianza legítima obliga a las autoridades públicas a actuar de manera coherente y no contradictoria con las partes privadas, especialmente cuando crean una expectativa razonable de que la autoridad pública seguirá actuando en consecuencia. Por lo tanto, el principio de confianza legítima constituye una garantía para el ciudadano frente a un cambio repentino e injustificado de la conducta continuada de las autoridades.

La confianza legítima que un particular, en este caso WhatsApp, deposita en la seriedad y estabilidad de las actuaciones administrativas, no solo es digna de protección y respeto, sino que requiere una conducta leal y honesta por parte de la Administración, volviéndose no sólo deseable desde un perspectiva moral, pero una institución jurídicamente vinculante.

Al respecto, la Corte Constitucional ha indicado :

> *"Por lo tanto, el principio de la buena fe exige a las autoridades y a los particulares mantener una coherencia en sus actuaciones, un respeto por los compromisos a los que se han obligado y una garantía de estabilidad y durabilidad de la situación que objetivamente permita esperar el cumplimiento de las reglas propias del tráfico jurídico"*

En términos similares, en la sentencia T-1094 de 2005, la Corte Constitucional señaló que :

> *"Este principio busca proteger al administrado frente a las modificaciones intempestivas que adopte la administración, desconociendo antecedentes en los cuales aquél se fundó para continuar en el ejercicio de una actividad o reclamar ciertas condiciones o reglas aplicables a su relación con las autoridades. Esto quiere decir que el principio de confianza legítima es un mecanismo para conciliar los posibles conflictos que surjan entre los intereses públicos y los intereses privados, cuando la administración ha creado expectativas favorables para el administrado y súbitamente elimina dichas condiciones. Así pues, la confianza que el administrado deposita en la estabilidad de la actuación de la administración, es digna de protección y debe respetarse (…)*

En síntesis, el principio de la confianza legítima es una expresión de la buena fe consistente en que el Estado no puede súbitamente alterar unas reglas de juego que regulaban sus relaciones con los particulares, sin que se les otorgue a estos últimos un período de transición para que ajusten su comportamiento a una nueva situación jurídica".

Finalmente, la Corte Constitucional también estableció que la administración pública tiene el deber de actuar en sus relaciones jurídicas con los particulares de manera consecuente con sus conductas precedentes, de manera que los administrados no se vean sorprendidos con conductas que, por ser contrarias, defrauden sus expectativas legítimamente fundadas" . De acuerdo con esta consideración general, cabe señalar que la confianza legítima de una parte puede formarse, no solo por

representaciones formales de las autoridades como, la cesión de un contrato, sino también por manifestaciones informales y conductas repetitivas de la Administración.

En el presente caso, si bien WhatsApp no reconoce que está sujeto a la Ley de Protección de Datos o que violó la Ley de Protección de Datos, incluso si la Resolución concluye erróneamente lo contrario, la SIC debe evitar el riesgo de violar arbitrariamente la confianza de WhatsApp.

Durante varios años, WhatsApp ha operado en Colombia sin haber recibido ningún aviso de incumplimiento de la Ley de Protección de Datos. Mientras tanto, WhatsApp ha proporcionado un flujo de consentimiento del usuario (es decir, información detallada y fácil de entender sobre la información que los usuarios están dando y sus derechos en relación con la autorización solicitada) que va muy por encima de la práctica de la industria y es consistente con el compromiso de WhatsApp con la privacidad. y transparencia. Por ejemplo, durante todo el proceso de actualización, WhatsApp ha proporcionado un amplio aviso y transparencia con respecto a la actualización. con diversos materiales informativos, como preguntas frecuentes y notificaciones en la aplicación (por ejemplo, las preguntas frecuentes antes mencionadas sobre los derechos de privacidad), que presentó de manera clara y accesible, los principales objetivos de la Actualización y las opciones de los usuarios.

A pesar de la transparencia de WhatsApp, la SIC nunca expresó ninguna creencia de que WhatsApp violara la Ley de Protección de Datos. Este enfoque creó una expectativa razonable en WhatsApp de que no se emitiría una orden contra esta entidad, ya que estaba cumpliendo con las leyes y regulaciones que son aplicables al Servicio de WhatsApp. Dado la cantidad de usuarios del servicio de WhatsApp con sede en Colombia (39 millones) y la publicidad de la Política de Tratamiento de Datos Personales y los Términos de servicio de WhatsApp, el SIC estaba al tanto de las actividades de WhatsApp en Colombia. Su inacción fue una fuerte señal de que la SIC no creía que fuera necesaria una investigación.

Luego, el 21 de enero de 2021, después de anunciar la actualización global de las Políticas de Tratamiento de Datos Personales de WhatsApp y de sus Términos de Servicios, WhatsApp recibió un requerimiento de información de la SIC, centrándose principalmente en la actualización. Pero esto aún no le dio a WhatsApp ninguna indicación de que el SIC había decidido repentinamente que WhatsApp violó las disposiciones de la Ley de Protección de Datos. Con base en el momento y el lenguaje del Requerimiento de la SIC, WhatsApp concluyó razonablemente que estaba motivado únicamente por la Actualización.

(…)

E. La Resolución es nula porque no cumple con el propósito de la Ley de Protección de Datos al no evidenciar que exista algún dato personal tratado en Colombia por WhatsApp para dar lugar a la aplicación de las facultades de la SIC.

La Resolución se basa en una suposición incorrecta: que WhatsApp trata datos personales en Colombia y que, por lo tanto, la Ley de Protección de Datos es aplicable a WhatsApp. Esta suposición llevó a una decisión que no cumple con el propósito de la Ley de Protección de Datos, por lo que WhatsApp respetuosamente solicita que la SIC la revoque.

En efecto, el Consejo de Estado ha determinado que un acto administrativo puede ser declarado nulo cuando se dicte sin prever el fin al que se le ha asignado la regulación.

En el presente caso, incluso si la Resolución se emitió correctamente (lo cual, como se describió anteriormente en las Secciones III.A, III.B y III.C, no lo fue), no logra el propósito (o se alinea con el espíritu) de las normas legales aplicables.

Primero, como se desprende del lenguaje del artículo 2 de la Ley de Protección de Datos, la Ley de Protección de Datos fue diseñada para regular el tratamiento de datos personales dentro del territorio colombiano. Como se describió anteriormente, WhatsApp no trata datos personales en Colombia. Por lo tanto, la Resolución no promueve significativamente el propósito legal de la Ley de Protección de Datos, ya que no puede regular el tratamiento de ningún dato personal fuera de Colombia. En cambio, la

Resolución alega una serie de deficiencias menores en la Política de Tratamiento de Datos Personales de WhatsApp (que la Compañía impugna como infundadas) para expandir masivamente la autoridad legal de la SIC, lo que no está permitido bajo el alcance de la Ley de Protección de Datos. Al respecto, reiteramos las consideraciones explicadas en los apartados III.A. y III.C, anterior, respecto a la incompetencia de la SIC para dictar la Resolución y el cumplimiento por WhatsApp de la Ley de Protección de Datos en todo caso.

En segundo lugar, la Resolución no opera dentro de los parámetros de la Ley de Protección de Datos según los cuales se aplicaría la autoridad de la SIC, ya que no evidencia que WhatsApp trate ningún dato personal en Colombia – como tal, no hay fundamento para que la SIC emita la Resolución bajo la Ley de Protección de Datos.

En efecto, la Resolución sobrepasa el alcance de la autoridad otorgada a la SIC bajo la Ley de Protección de Datos sin lograr el propósito (o reflejar el espíritu) de dicha ley y por lo tanto, la SIC debe revocarla.

F. El requisito de la Resolución de que WhatsApp se registre en el Registro Nacional de Bases de Datos (RNBD) es procesal y sustantivamente inválido.

Por las razones jurisdiccionales, procesales y sustantivas descritas anteriormente en las Secciones III.A, III.B y III.C, se debe revocar la orden de la Resolución de que WhatsApp registre sus bases de datos en el RNBD.

El artículo 25 de la Ley de Protección de Datos establece que : "El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país. El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos. Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley" (Énfasis propio).

Para sustentar su orden, la SIC cita el Decreto 90 de 18 de enero de 2018, que modificó el Decreto 1074 de 2015, el reglamento que implementa el artículo 25 de la Ley Protección de Datos, que exige que "Sociedades y entidades sin ánimo de lucro que tengan activos totales superiores a 100.000 Unidades de Valor Tributario (UVT)" registren sus bases de datos. Sin ningún análisis, la SIC concluye que WhatsApp está sujeto a este requisito.

Pero la SIC, respetuosamente, no tiene jurisdicción ni competencia para emitir tal requisito, ya que WhatsApp no trata datos dentro de Colombia. Y la SIC no mencionó en absoluto este requisito en su requerimiento de información, negando así a WhatsApp cualquier oportunidad de impugnar la aplicabilidad de este requisito (violando sus derechos de debido proceso). Finalmente, como cuestión de fondo, la orden de la SIC se basa en evidencia insuficiente, ya que nunca investigó adecuadamente si los activos de WhatsApp en Colombia superan las 100.000 UVT; de haberlo tenido, la SIC se habría enterado de que WhatsApp no tiene activos en Colombia.

Asimismo, considerando el texto y el propósito del artículo 25, es claro que la ley no debe aplicarse a una entidad extranjera como WhatsApp. De hecho, la métrica UVT de la Ley Protección de Datos tiene su origen en la Ley 905 de 2004, que regula a las micro, pequeñas y medianas empresas colombianas. El Decreto 90 de 18 de enero de 2018 modificó el Decreto 1074 de 2015 para determinar qué entidades deben cumplir con esta obligación con base en esta Ley, la cual está claramente dictada en el contexto colombiano, para las empresas colombianas. Esto refleja claramente que dicha ley y regulación está destinada a aplicarse a las empresas colombianas que tienen activos en Colombia, en lugar de a las extranjeras.

Aplicar la métrica UVT a activos fuera del país la descontextualizaría, ya que las empresas constituidas en otros países que tienen activos en otros países se rigen por otras leyes.

Si se acepta el argumento jurisdiccional de la Resolución basado en cookies, cualquier entidad (incluidas las entidades gubernamentales) que tenga un sitio web que utilice cookies accesibles en Colombia y más de 100,000 UVT en activos, necesitaría registrarse en el RNBD en Colombia. Esta es una expansión dramática de la autoridad que daría como resultado resultados absurdamente desproporcionados para las partes reguladas, los consumidores y también la propia SIC. De la nada, los deberes regulatorios de la SIC ahora incluirían millones de entidades en todo el mundo, y el RNBD se expandiría astronómicamente en tamaño. Sin embargo, la SIC no está publicando órdenes contra esos millones de entidades en todo el mundo, lo que genera claramente un desequilibrio contra WhatsApp que es difícil de entender dada la percepción y aceptación del Servicio de WhatsApp entre los usuarios en Colombia.

Para evitar este resultado extremo y por ser erróneo, respetuosamente le solicitamos a la SIC que también revoque esta parte de la Resolución.

G. WhatsApp no está obligado a contar con una dirección de correo electrónico para notificaciones electrónicas.

El artículo 4 de la Resolución exhorta a WhatsApp a proporcionar a la SIC una dirección de correo electrónico en la que pueda recibir comunicaciones o notificaciones de actos administrativos. WhatsApp informa respetuosamente a la SIC que no es una entidad constituida en Colombia y no tiene la obligación legal de crear o designar una dirección de correo electrónico para notificaciones electrónicas, según lo establecido en el artículo 291 del CGP.

WhatsApp solicita respetuosamente ser notificado en 1601 Willow Road Menlo Park, California, Estados Unidos, de acuerdo con los tratados internacionales aplicables (y para garantizar el derecho de WhatsApp al debido proceso)".

TERCERO. 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 29826 del 19 de mayo del 2021**, se procede a resolver el recurso de reposición, de acuerdo con las siguientes:

CONSIDERACIONES DE LA DIRECCIÓN DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES

1. COOKIES: RECOLECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

La sociedad recurrente afirma lo siguiente:

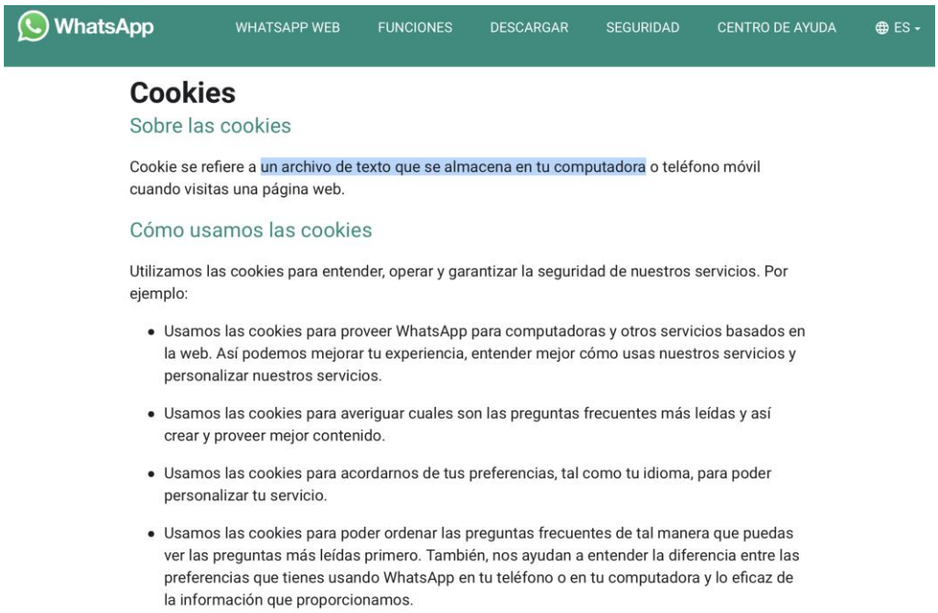
"Como punto de partida, WhatsApp rechaza la premisa de que sus actividades de tratamiento de datos personales (a través de cookies o de otro cualquier otro modo) se realicen en Colombia y que utilice medios situados en el territorio colombiano para el tratamiento de datos personales. Todos los actos de tratamiento de datos personales se realizan en los servidores de WhatsApp, los cuales están ubicados fuera del territorio colombiano, por lo que, de conformidad con el artículo 2 de la Ley de Protección de Datos, no hay jurisdicción sobre dichas actividades de tratamiento.

El hecho de que WhatsApp pueda utilizar cookies para el funcionamiento de la versión web de su aplicación (la cual, como se explicó anteriormente es una función complementaria y no es necesaria para operar el servicio) o del sitio web de WhatsApp no cambia la premisa fundamental de que el tratamiento de datos personales subyacente para prestar el servicio de WhatsApp, incluido el relacionado con cualquier dato asociado a una cookie, se realiza fuera del territorio colombiano".

Al respecto, esta autoridad destaca lo siguiente sobre las *web cookies.*

En primer lugar, la compañía WhatsApp LLC define el término *cookie*, en su Política de Privacidad[9] de la siguiente manera:

[9] Obtenido en https://www.whatsapp.com/legal/cookies



WhatsApp WHATSAPP WEB FUNCIONES DESCARGAR SEGURIDAD CENTRO DE AYUDA ES

Cookies

Sobre las cookies

Cookie se refiere a un archivo de texto que se almacena en tu computadora o teléfono móvil cuando visitas una página web.

Cómo usamos las cookies

Utilizamos las cookies para entender, operar y garantizar la seguridad de nuestros servicios. Por ejemplo:

- Usamos las cookies para proveer WhatsApp para computadoras y otros servicios basados en la web. Así podemos mejorar tu experiencia, entender mejor cómo usas nuestros servicios y personalizar nuestros servicios.
- Usamos las cookies para averiguar cuales son las preguntas frecuentes más leídas y así crear y proveer mejor contenido.
- Usamos las cookies para acordarnos de tus preferencias, tal como tu idioma, para poder personalizar tu servicio.
- Usamos las cookies para poder ordenar las preguntas frecuentes de tal manera que puedas ver las preguntas más leídas primero. También, nos ayudan a entender la diferencia entre las preferencias que tienes usando WhatsApp en tu teléfono o en tu computadora y lo eficaz de la información que proporcionamos.

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

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

Veamos:

En el caso de la República Oriental del Uruguay, la Unidad Reguladora y de Control de Datos Personales señala lo siguiente en su guía sobre "Cookies y perfiles"[10]:

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

En el Reino de España, la Agencia Española de Protección de Datos señala lo siguiente en su "Guía sobre el uso de cookies"[11]:

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

[10] República Oriental del Uruguay, Unidad Reguladora y de Control de Datos Personales. *Cookies y perfiles*. En: https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/documentos/publicaciones/Guia%2Bcookies%2By%2Bperfiles.pdf
[11] Reino de España. Agencia Española de Protección de Datos . Guía sobre el uso de cookies. En: https://www.aepd.es/es/documento/guia-cookies.pdf

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

En la República de Irlanda, la Oficina del Comisionado de Protección de Datos publicó en el 2020 su guía sobre "Cookies y otras tecnologías de seguimiento"[12]. En ella, se afirmó que:

"*Las cookies* ***suelen ser pequeños archivos de texto almacenados en un dispositivo, como una PC****, un dispositivo móvil o cualquier otro dispositivo que pueda almacenar información. Los dispositivos que pueden utilizar cookies también incluyen los llamados dispositivos de "Internet de las cosas" (IoT) que se conectan a Internet.*

Las cookies cumplen una serie de funciones importantes, que incluyen recordar a un usuario y sus interacciones anteriores con un sitio web. Se pueden usar, por ejemplo, para realizar un seguimiento de los artículos en un carrito de compras en línea o para realizar un seguimiento de la información cuando ingresa detalles en un formulario de solicitud en línea. Las cookies de autenticación también son importantes para identificar a los usuarios cuando inician sesión en servicios bancarios y otros servicios en línea

(…)

La información almacenada en las cookies puede incluir datos personales, como una dirección IP, un nombre de usuario, un identificador único o una dirección de correo electrónico. *Pero también puede contener datos no personales como configuraciones de idioma o información sobre el tipo de dispositivo que una persona está usando para navegar por el sitio".* (Énfasis añadido).

En el Reino Unido de Gran Bretaña e Irlanda del Norte, la Oficina de la Comisión de Información publicó su "Guía sobre el uso de cookies y tecnologías similares"[13], en la cual se afirma lo siguiente:

"**Qué son cookies?**
Las cookies son pequeños fragmentos de información, que normalmente constan de letras y números, que los servicios en línea proporcionan cuando los usuarios los visitan. El software en el dispositivo del usuario (por ejemplo, un navegador web) puede almacenar cookies y enviarlas al sitio web la próxima vez que lo visite.

¿Cómo se utilizan las cookies?

Las cookies son una tecnología específica que almacena información entre visitas al sitio web. Se utilizan de diversas formas, como por ejemplo:

- *recordar lo que hay en una "cesta" al comprar productos en línea;*
- *ayudar a los usuarios a iniciar sesión en un sitio web;*
- *analizar el tráfico de un sitio web; o*
- *seguimiento del comportamiento de navegación de los usuarios.*

Las cookies pueden ser útiles porque permiten que un sitio web reconozca el dispositivo de un usuario. Se utilizan ampliamente para hacer que los sitios web funcionen o funcionen de manera más eficiente, así como para proporcionar información a los editores del sitio. Sin cookies, o algún otro método similar, los sitios web no tendrían forma de "recordar" nada sobre los visitantes, como cuántos artículos hay en una cesta de compras o si han iniciado sesión."

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

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

La Oficina Garante de la protección de datos personales de la República de Italia publicó este año (2021) sus Directrices para *cookies* y otras herramientas de seguimiento[14], en donde señalan, entre otras, lo siguiente:

> *"**Las cookies son, por regla general, cadenas de texto que los sitios web visitados por el usuario** (los llamados sitios web de 'editores' o 'propios') o diferentes sitios web o servidores web (los llamados 'terceros') **colocan y almacenan en un dispositivo terminal en posesión***
>
> ***del usuario**, ya sea directamente, como es el caso de los sitios web de los editores, o indirectamente, como es el caso de los "terceros", es decir, a través de la intermediación de los sitios web de los editores.*
>
> ***Los dispositivos terminales a los que se hace referencia incluyen, por ejemplo, un ordenador, una tableta, un teléfono inteligente o cualquier otro dispositivo capaz de almacenar información**. (…)*
> *(…)*
>
> ***La información codificada en las cookies puede incluir datos personales, como una dirección IP, un nombre de usuario, un identificador único o una dirección de correo electrónico**, pero también puede incluir datos no personales como la configuración de idioma o información sobre el tipo de dispositivo que está usando una persona para navegar dentro del sitio web.*
>
> *Por lo tanto, las cookies pueden realizar funciones importantes y diversas, **incluido el seguimiento de la sesión, el almacenamiento de información de acceso al servidor específica relacionada con la configuración del usuario, facilitar el uso de contenido en línea, etc.** Por ejemplo, se pueden utilizar para realizar un seguimiento de los elementos en una cesta de la compra en línea o la información utilizada para completar un formulario informático".* (Énfasis añadido).

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

> "*Una cookie es información guardada por su navegador web. Cuando usted visita un sitio web, el sitio puede colocar una cookie en su navegador web para que pueda reconocer su dispositivo en el futuro. Si regresa a ese sitio más adelante, puede leer esa cookie para recordarlo de su última visita y realizar un seguimiento de usted a lo largo del tiempo.*
> ***Usos***
>
> - ***Recopilar información sobre las páginas que ve y sus actividades en el sitio***
> - ***Permitir que el sitio lo reconozca**, por ejemplo:*
>   - *Recordando su ID de usuario*
>   - *Ofreciendo un carrito de compras en línea*
>   - *Realizar un seguimiento de sus preferencias si vuelve a visitar el sitio web*
> - *Personaliza tu experiencia de navegación*
> - *Entregar anuncios dirigidos a usted*" [15]. (Énfasis añadido).

La FTC público la guía "*Cómo Proteger tu Privacidad en línea*"[16], en donde afirma lo siguiente:

> ***"Lo que hay que saber acerca del rastreo en línea***
>
> ***Cookies***

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

[15] United States. Federal Trade Commission. What are cookies? En: https://www.ftc.gov/site-information/privacy-policy/internet-cookies Consultada el 16 de septiembre de 2021.

[16] Estados Unidos de América. Comisión Federal de Comercio. El texto completo de la guía puede consultarse en: https://www.consumidor.ftc.gov/articulos/como-proteger-su-privacidad-en-linea

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

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

Los sitios web que usted visita suelen permitir que otras compañías también coloquen cookies, por ejemplo, para mostrarle anuncios personalizados o dirigidos de acuerdo a sus

intereses. Estas son ***cookies de terceros****. A continuación, algunos ejemplos de cookies de terceros:*

- *Una compañía de publicidad le coloca una cookie y ve que usted visitó un sitio web sobre carreras a pie. Entonces, cuando usted visita otros sitios web, le muestra un anuncio de calzado deportivo para correr.*
- *Una compañía analítica usa una cookie para obtener detalles sobre su visita a un sitio web, por ejemplo, cuánto tiempo pasó en ese sitio y qué paginas visitó. Puede usar la información que recolecta para detectar problemas con el sitio y mejorarlo."* (Énfasis fuera de texto).

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

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

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

(…)

Con carácter preliminar ha de precisarse que, según las indicaciones que figuran en la resolución de remisión, ***las cookies que pueden colocarse en el equipo terminal de los usuarios*** *que participan en el juego con fines promocionales organizado por Planet49 llevan un número que se adjudica a los datos de registro de dicho usuario, quien debe inscribir su nombre y su dirección en el formulario de participación de dicho juego. El órgano jurisdiccional remitente añade que la asociación* ***de ese número y esos datos personaliza los datos***

almacenados por las cookies cuando el usuario se sirve de Internet, de modo que la recogida de tales datos mediante las cookies constituye un tratamiento de datos personales. *Estas indicaciones fueron confirmadas por Planet49, quien subrayó en sus observaciones escritas que el consentimiento correspondiente a la segunda casilla constituye una autorización de recogida y tratamiento de datos personales, y no de información anónima.*

Una vez realizadas estas precisiones, procede señalar que, conforme al artículo 5, apartado 3, de la Directiva 2002/58, los Estados miembros velarán por que únicamente ***se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un usuario*** *cuando dicho usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en*

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

particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46". (Énfasis añadido).

2. APLICACIÓN DE LA LEY 1581 DE 2012 CUANDO SE RECOLECTAN DATOS PERSONALES EN EL TERRITORIO DE LA REPÚBLICA DE COLOMBIA A TRAVÉS DE *COOKIES* QUE SE INSTALAN EN LOS EQUIPOS O DISPOSITIVOS DE LAS PERSONAS RESIDENTES O DOMICILIADAS EN ESTE TERRITORIO

Sobre la aplicación de la Ley 1581 de 2012 a la sociedad recurrente, en el escrito de reposición aquella manifiesta lo siguiente:

> *"Ese alcance es incompatible con el ámbito territorial pretendido por la Ley de Protección de Datos, y conduciría a una aplicación de la Ley de Protección de Datos que sobrepasa todos los límites territoriales y de soberanía. Si la ley pretendiera un alcance tan global, lo habría dicho claramente; en cambio, prevé un alcance más estrecho y matizado para el tratamiento de datos personales que verdaderamente se lleva a cabo dentro de Colombia. De hecho, esta interpretación haría que la segunda cláusula del artículo 2 fuera redundante porque nunca sería necesario basarse en tratados internacionales para aplicar la Ley de Protección de Datos a entidades extranjeras si el "tratamiento de datos" se interpretara de manera tan amplia. Claramente, la interpretación de la Resolución es irrazonable y defectuosa, y, respetuosamente, la SIC no tenía jurisdicción para emitir la Resolución*".

La motivación de competencia que esta autoridad presentó en la resolución recurrida es acorde con la Constitución, la ley y la jurisprudencia de la República de Colombia. Resulta pertinente poner de presente lo siguiente dado que la compañía pone en duda la competencia de esta entidad respecto de WhatsApp LLC:

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

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

El artículo 15 de la Constitución Política Colombiana, por su parte, establece el Derecho Fundamental al debido Tratamiento de Datos personales, de la siguiente manera:

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

Nótese como para la propia Constitución de la República de Colombia es importante la **recolección** y el **Tratamiento** de Datos sin que sea relevante si la misma se realiza mediante mecanismos manuales, automatizados o si se recurre al uso de tecnologías conocidas o por conocer para dicho efecto. Para la Constitución lo determinante es que la recolección o el tratamiento de datos no se haga de cualquier manera sino respetando la libertad y demás garantías establecidas en la misma.

Como es sabido, el literal g) de su artículo 3 de la Ley Estatutaria 1581 de 2012 define Tratamiento como, "***Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección****, almacenamiento, uso, circulación o supresión".* (Énfasis añadido).

El significado legal de Tratamiento tiene varias características:

En primer lugar, es omnicomprensiva porque incluye toda actividad, operación o conjunto de operaciones sobre Datos personales. Además, no se limita a los ejemplos enunciativos del citado concepto legal, sino que, abarca cualquier otro que involucre directa o indirectamente el uso, almacenamiento o circulación de Datos personales. Sobre este punto, la Corte Constitucional señaló en el numeral 2.5.9. de la Sentencia C-748 de 2011 que, "*lo que se pretende con este proyecto es que* ***todas las operaciones o conjunto de operaciones con los datos personales quede***

***regulada por las disposiciones del proyecto de ley en mención**, con las salvedades que serán analizadas en otro apartado de esta providencia*". (Destacamos).

En segundo lugar, la operación o conjunto de operaciones sobre Datos personales puede ser realizada directa o indirectamente por una o varias personas de forma tal que, en un Tratamiento de Datos personales pueden existir varios Responsables o corresponsables. Debe precisarse que, no es necesario que todas las etapas del Tratamiento las realice una misma empresa u organismo. Puede ser un Tratamiento diseñado por una organización en la que se divide el trabajo para alcanzar ciertos objetivos, pero, al final, unos y otros son Responsables y corresponsables del Tratamiento de Datos personales.

En tercer lugar, es neutral tecnológicamente porque cobija el Tratamiento realizado mediante cualquier medio físico o electrónico como, entre otras, las *cookies.* WhatsApp LLC realiza Tratamiento de Datos personales en territorio colombiano porque usa *cookies* para recolectar Datos personales en el territorio de la República de Colombia. Razón suficiente, para que de conformidad con lo establecido en el artículo 2 de la Ley Estatutaria 1581 de 2012 cumpla con lo estipulado en dicha ley y sus normas reglamentarias.

Como se señaló, el artículo 2 de la Ley Estatutaria 1581 de 2012 ordena que ***"La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano** o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales*". (Énfasis añadido). El término "Tratamiento" no solo se menciona en el artículo 15 de la Constitución Política de la República de Colombia, sino que, es determinante para establecer el campo de aplicación de la citada ley, la cual lo define de la siguiente manera:

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

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

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

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

En el presente caso, WhatsApp LLC está dentro de lo señalado en el literal a) porque usa *cookies* para recolectar o realizar Tratamiento Datos personales en el Territorio de la República de Colombia.

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 personales. Por lo tanto, quien recolecta y trata Datos personales en el territorio colombiano, debe cumplir la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias.

Como se vio, la Ley 1581 de 2012 fija de manera expresa su ámbito de aplicación "*al tratamiento de datos personales efectuado **en territorio colombiano**".*

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

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

La sociedad recurrente afirma que:

> "*De acuerdo con los claros términos del referido artículo 2 y los principios de soberanía internacional, instamos respetuosamente a la SIC a que revoque la Resolución, ya que extiende la autoridad de la SIC bajo la Ley de Protección de Datos para alcanzar cualquier sitio web al que se acceda desde Colombia y que utilice cookies. Como se describe más adelante, dada la omnipresencia del uso de cookies en todo el mundo, esto efectivamente otorga a la SIC jurisdicción global e ilimitada, violando tanto los términos de la Ley Protección de Datos como la soberanía de otras naciones"*.

La ley colombiana **no distingue si el Tratamiento se debe hacer de determinada manera ni excluye ninguna forma, herramienta, tecnología o proceso para recolectar o tratar datos personales en el territorio colombiano**. De esta manera, si se recolectan o tratan Datos en el territorio colombiano aplica la ley colombiana.

No debe olvidarse que existe un principio general de interpretación jurídica según el cual **en donde la ley no distingue, no le es dado al intérprete hacerlo**. Principio que en este caso resulta plenamente aplicable porque WhatsApp LLC realiza Tratamiento de Datos en el territorio colombiano mediante el uso web cookies. Si la ley colombiana no distingue la forma ni los mecanismos como se realiza el Tratamiento en el territorio colombiano, pues no le corresponde a esta autoridad excluir el uso de este como una de tales herramientas.

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

- CORTE SUPREMA DE JUSTICIA. SALA DE CASACIÓN PENAL. AUTO INTERLOCUTORIO DE 3 DE MAYO DE 2017 (AP2789-2017. RADICACIÓN N.° 49891. APROBADO ACTA N.º 124) MP. DR. FERNANDO ALBERTO CASTRO CABALLERO[18].: " ***Acorde con el principio interpretativo que reza que donde la ley no distingue no le es dado al interprete hacerlo****, se concluye que si la Ley 1820 no excluyó de manera explícita como destinatarios de sus preceptos a los ex integrantes de las FARC - EP, por ejemplo a causa de anterior desmovilización en los términos de la Ley 975 de 2005 u otra normatividad, mal podría haberlo hecho como lo hizo en este caso la Sala de Justicia y Paz del Tribunal Superior de Bogotá*"

- CORTE CONSTITUCIONAL, SENTENCIA C-317 DEL 3 DE MAYO DE 2012. MP. DRA MARÍA VICTORIA CALLE CORREA[19]. "*Al respecto la Corte considera que* ***no le asiste razón al demandante*** *pues si bien la Constitución contiene una atribución expresa de representación gubernamental para la iniciativa legislativa en cabeza de los Ministros, y no una atribución similar para la iniciativa constituyente,* ***resulta plenamente aplicable al tema, el principio general de interpretación jurídica según el cual donde la norma no distingue, no le corresponde distinguir al intérprete****, no resultando jurídicamente viable deducir, por esta vía, reglas constitucionales implícitas que contrarían el texto mismo del artículo 208 Superior, cuyo mandato general de vocería gubernamental no establece tal diferenciación*." (Énfasis añadido)

- CORTE CONSTITUCIONAL, SENTENCIA C-127 DE 22 DE ABRIL DE 2020. MP. DRA. CRISTINA PARDO SCHLESINGER[20].: "*Por lo anterior,* ***en desarrollo del principio general de interpretación jurídica según el cual donde la norma no distingue, no le corresponde distinguir al intérprete****, no resulta viable deducir la existencia de la regla de exclusión implícita a que aluden los demandantes*." (Énfasis añadido).

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

---

[18] El texto puede leerse en: En: https://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b2may2017/AP2789-2017.pdf
[19] El texto completo de la sentencia puede consultarse en: https://www.corteconstitucional.gov.co/relatoria/2012/C-317-12.htm
[20] La sentencia puede consultarse en: https://www.corteconstitucional.gov.co/Relatoria/2020/C-127-20.htm

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

En conclusión, **WhatsApp LLC** mediante mecanismos electrónicos recolecta Datos personales en el territorio de la República de Colombia. Por ende, ese Tratamiento de Datos personales está sujeto a la legislación colombiana. En virtud de lo anterior, no asiste razón a apoderada en cuanto a que no le es aplicable la Ley Estatutaria 1581 de 2012.

4. DE LA ORDEN EMITIDA, SU CUMPLIMIENTO Y DEBIDO PROCESO

Como es sabido, en el artículo 19 de la Ley Estatutaria 1581 de 2012, 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, existen expresas y suficientes facultades legales para que esta autoridad pueda impartir órdenes o instrucciones.

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

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

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

No sobra recordar **que las órdenes no son sanciones porque según la Ley 1581 de 2012 sólo son sanciones las señaladas en el artículo 23, a saber**:

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

De otra parte, es relevante destacar que no se violó el debido proceso por las siguientes razones:

- Esta Dirección no desconoció el principio de legalidad, sino que, aplicó lo que ordena la ley colombiana. Nos remitimos a los fundamentos constitucionales, legales y tecnológicos señalados, lo largo de este acto.
- De la lectura del acto administrativo recurrido se puede constatar que el acto fue suficientemente motivado conforme con la regulación colombiana.
- En el expediente reposa evidencia de las comunicaciones realizadas a WhatsApp LLC para que ejerza su derecho de defensa. Como fruto de lo anterior, dicha empresa: i) allegó respuesta a esta entidad a la comunicación remitida en enero del 2021, y ii) presentó el recurso de reposición y apelación con sus argumentos y pruebas que han sido analizados para adoptar la decisión recurrida y el presente acto administrativo.
- La diligencia y el cumplimiento del debido proceso por parte de esta entidad ha quedado acreditado en el expediente y la motivación de la decisión adoptada.

Es así como durante el procedimiento administrativo pudo la sociedad recurrente, entre otras, hacer lo siguiente:

- Dar respuesta o guardar silencio frente a los requerimientos de esta autoridad.
- Aportar documentos que respalden sus afirmaciones.
- Solicitar pruebas en el proceso.
- Rendir descargos.
- Presentar el recurso de reposición y en subsidio de apelación.

Debe resaltarse que 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 21-11032 en todo momento, y desde el inicio de la investigación ha estado a disposición de la sociedad recurrente, para que sea consultado; 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'*"[21] (Destacamos)

Así las cosas, vale la pena llamar la atención sobre el hecho de que **WhatsApp LLC** siempre tuvo la oportunidad de expresar su opinion, controvertir las pruebas y de acceder al expediente. No

[21] 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.

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, el recurso de reposición en subsidio de apelación interpuesto por la sociedad recurrente es otra alternativa prevista por la Ley 1437 de 2011 para debatir las conclusiones del acto administrativo definitivo que pone fin a la investigación en curso. Esta posibilidad está en el artículo 74 de la Ley 1437 de 2011:

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

Luego de emitido el acto administrativo, es la sociedad recurrente la que tiene la potestad - *que no es obligatoria*-, de interponer los recursos señalados en el artículo referido y aportar con estos las pruebas que pretende hacer valer.

Así, por medio del presente acto administrativo se analiza el recurso de reposición interpuesto por la sociedad recurrente donde tienen la oportunidad de controvertir las conclusiones y pruebas consideradas en el acto recurrido. De esta manera, la recurrente ha contado con todas las oportunidades de ley para ejercer su derecho de defensa, la inconformidad con el resultado de la presente actuación de ninguna manera, significan que esta entidad haya vulnerado el derecho fundamental al debido proceso.

Se reitera que esta autoridad:

1. Garantizó el derecho de la sociedad a ser oída, aportar y solicitar pruebas; y,
2. Garantizó el derecho de defensa y contradicción, a lo largo de la actuación y con el análisis del recurso en cuestión.

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

5. NOTIFICACIÓN DEL ACTO ADMINISTRATIVO RECURRIDO

Esta Superintendencia de Industria y Comercio notificó acorde a lo establecido en la legislación colombiana a la sociedad recurrente. Lo anterior, puede evidenciarse a continuación.

Primero, el diez y nueve (19) de mayo de 2021 esta Superintendencia de Industria y Comercio, por medio de la Secretaría General, remitió a la dirección 1601 Willow Road Menlo Park, California, Estados Unidos, una citación de notificación en donde se le informó los siguiente:

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

RADICACION: 21-11032- -8	**FECHA: 2021-05-19 14:12:11**
TRAMITE: 384 PROTECDATOS	**EVENTO: 330 INVESTIGACION**
ACTUACION: 432 COMUNICACTOADM	**FOLIOS: 1**
DEPENDENCIA: 7100 DIRINVDATOSPERS	

CITACIÓN NOTIFICACIÓN

Señor(a)(es)
WHATSAPP LLC
1601 Willow Road Menlo Park, California 94025
MENLO PARK - CALIFORNIA
ESTADOS UNIDOS DE AMERICA

Referencia	Resolución 29826
Fecha:	19 de mayo de 2021
Expediente:	21-11032-
Trámite:	384 PROTECCION DE DATOS PERSONALES
Evento:	330 INVESTIGACION
Actuación:	432 COMUNICACION ACTO ADMINISTRATIVO

De conformidad con lo establecido en el Decreto Presidencial 491 del 28 de marzo de 2020 y con el fin de notificarle el contenido del acto administrativo de la referencia, de manera atenta solicito realizar el registro para notificación personal electrónica en la página web www.sic.gov.co, a través de la opción "Notificaciones"- "Notificaciones Electrónicas" o enviando correo electrónico a contactenos@sic.gov.co asunto "Autorización Notificación Personal Electrónica".

Si no se surte la notificación personal electrónica dentro de los 5 días hábiles siguientes a la recepción de esta citación, esta se realizará por medio de aviso según lo dispuesto en el artículo 69 de la Ley 1437 de 2011 que se remitirá a su correo electrónico, con copia íntegra de la decisión.

Lo invitamos a evaluar el proceso de notificación y comunicación de actos administrativos de la Superintendencia de Industria y Comercio, en la página web www.sic.gov.co, opción notificaciones, seleccionando "Encuesta de satisfacción".

Posteriormente, ante la ausencia de una notificación personal electrónica 5 días hábiles siguientes a la recepción de aquella citación, se le remitió a la sociedad el día siete (7) de julio de 2021 una notificación por aviso en los siguientes términos:

NOTIFICACIÓN POR AVISO

Doctor(a)
WHATSAPP LLC
1601 Willow Road Menlo Park, California 94025
MENLO PARK - CALIFORNIA
ESTADOS UNIDOS DE AMERICA

Asunto: Radicación: 21-11032- -9
Trámite: 384 PROTECCION DE DATOS PERSONALES
Evento: 330 INVESTIGACION
Actuación: 846 NOTIFICACION POR AVISO
Folios: 1

Aviso No. **15032** Fecha del Aviso: **06/07/2021**
RESOLUCIÓN **29826** Fecha: **19/05/2021**

LA SECRETARÍA GENERAL
HACE SABER:

Que ésta superintendencia profirió el acto administrativo relacionado anteriormente, del cual se entrega copia íntegra adjunta al presente aviso, en el que indica en su parte resolutiva la autoridad que lo expidió, los recursos que legalmente proceden, las autoridades ante quienes deben interponerse y los plazos respectivos, de conformidad con lo establecido en el artículo 69 de la Ley 1437 de 2011.

SE INFORMA QUE LA NOTIFICACIÓN QUE POR ESTE MEDIO SE HACE SE CONSIDERARÁ SURTIDA AL FINALIZAR EL DÍA SIGUIENTE AL DE LA ENTREGA DEL AVISO EN EL LUGAR DE DESTINO.

Lo invitamos a evaluar el proceso de notificación y comunicación de actos administrativos de la Superintendencia de Industria y Comercio, en la página web www.sic.gov.co, opción notificaciones, seleccionando "Encuesta de satisfacción", o a través del siguiente código QR:

Es así como, de acuerdo en lo establecido previamente, el Grupo de Notificación y Certificaciones de esta Superintendencia de Industria y Comercio expide la siguiente certificación:

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO	
RAD: 21-11032- -10	FECHA: 2021-07-26 13:13:42
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 29826 de fecha 19/05/2021 proferido en el expediente 21-11032, 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
WHATSAPP LLC	N.A.	Aviso	15032	16/07/2021

Se expide a los veintiséis (26) dia(s) del mes de julio de dos mil veintiuno (2021), con destino a DIRECCIÓN DE INVESTIGACIÓN DE PROTECCIÓN DE DATOS PERSONALES .

ALEJANDRO COY QUINTERO
COORDINADOR GRUPO NOTIFICACIONES Y CERTIFICACIONES

De esta manera, queda en evidencia como la Superintendencia de Industria y Comerció notificó el acto administrativo recurrido de acuerdo con la legislación colombiana. Respetando, en todo momento, el derecho fundamental al debido proceso en cabeza de la sociedad WhatsApp LLC.

6. LOS RESPONSABLES DEL TRATAMIENTO TIENEN LA CARGA DE PROBAR EL CUMPLIMIENTO DE SUS DEBERES LEGALES

La sociedad recurrente afirma en su escrito que, "*la Resolución desconoce la presunción de inocencia de WhatsApp contenida en el artículo 29 de la Constitución Política*".

Esta Dirección no puede estar más en desacuerdo con dicha afirmación. Precisamente, la regulación colombiana sobre Tratamiento de datos 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[22]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)

Adicionalmente, de la lectura de la Ley Estatutaria 1581 de 2012 y sus decretos reglamentarios se advierten las siguientes cargas probatoria:

- Acreditar prueba de la autorización del Titular del dato[23].
- Demostrar que se informó lo que ordena el parágrafo del artículo 12 de dicha ley
- Suministrar una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso[24].
- Documentar los procedimientos para el tratamiento, conservación y supresión de los datos personales de conformidad con las disposiciones aplicables a la materia de que se trate[25].
- Desarrollar sus políticas para el tratamiento de los datos personales y velar porque los encargados del tratamiento den cabal cumplimiento a las mismas[26].
- Conservar el modelo del aviso de privacidad que utilicen para cumplir con el deber que tienen de dar a conocer a los titulares la existencia de políticas del tratamiento de la información y la forma de acceder a las mismas, mientras se traten datos personales conforme al mismo y perduren las obligaciones que de este se deriven[27].
- Adoptar las medidas razonables para asegurar que los datos personales que reposan en las bases de datos 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[28].

En el presente caso, no estamos frente a una investigación mediante la cual se esté estableciendo la eventual responsabilidad penal de una persona.

Bajo estas premisas, la recurrente estaba en el deber de demostrarle a esta Superintendencia de Industria y Comercio el cumplimiento de los deberes legales. Esto es, aquellos establecidos en la comunicación remitida por parte de esta autoridad el doce (12) de enero del 2021[29]:

---

[22] Incorporado en el Decreto 1074 de 2015
[23] Cfr. Literal b) del artículo 17 de la Ley 1581 de 2012
[24] Artículo 4 del Decreto 1377 de 2013.
[25] Artículo 11 del Decreto 1377 de 2013.
[26] Artículo 13 del Decreto 1377 de 2013.
[27] Artículo 16 del Decreto 1377 de 2013.
[28] Artículo 22 del Decreto 1377 de 2013.
[29] Documento con número de radicado 21-11032- -0-0.

I. Establecer si las *Políticas de Privacidad* de WhatsApp, los *Términos de Servicio* y el Tratamiento de Datos personales efectuado en este territorio por parte de esa compañía están cumpliendo con la regulación colombiana en la materia; y
II. Verificar la implementación del Principio de Responsabilidad Demostrada (artículos 26 y 27 del Decreto 1377 de 2013 incorporado en el Decreto 1074 de 2015).

Entonces, la resolución recurrida no desconoce la presunción de inocencia de WhatsApp contenida en el artículo 29 de la Constitución Política.

7. SOBRE EL PRESUNTO CUMPLIMIENTO DE WHATSAPP LLC DE LA LEY 1581 DE 2012 Y SUS DECRETOS REGLAMENTARIOS

La sociedad recurrente, en su escrito de reposición afirma lo siguiente:

> "*La Resolución concluye que WhatsApp no cumple con los requisitos de la Ley de Protección de Datos (que en cualquier caso no se aplica a las prácticas de datos de WhatsApp, como se detalla anteriormente). Por el contrario, a pesar de no estar obligado a cumplir con la ley colombiana, De hecho, la Política de Tratamiento de Datos Personales de WhatsApp de hecho incluye los requisitos mencionados en la orden y ha adoptado medidas de cumplimiento de la privacidad a nivel mundial*".

Al respecto, es importante señalar que, del análisis realizado por esta autoridad en la resolución recurrida, se puede concluir que dichas afirmaciones no son ciertas. Sobre aquella labor de verificación realizada por esta Dirección, es importante destacar lo siguiente:

a. Esta Autoridad tiene amplias facultades legales para verificar el cumplimiento del régimen general de protección de Datos personales, lo cual incluye lo establecido en la Ley Estatutaria 1581 de 2012 y sus demás normas reglamentarias. Por lo que, si esta entidad lo considera necesario también se cerciorará del cumplimiento de los requisitos de la Política de Tratamiento de la Información de cualquier compañía que realice Tratamiento de Datos personales en el territorio de la República de Colombia.
b. En la valoración no se está dando ningún tipo de peso o "puntaje" a cada deber como equivocadamente lo afirma el apoderado. Pues, en todo caso, la investigada debe tener claro que TODOS LOS DEBERES Y OBLIGACIONES LEGALES SON IGUAL DE IMPORTANTES. Lo que se hizo fue desglosar uno a uno los puntos establecidos en la norma con el propósito de dar mayor claridad y lograr que el destinatario de la orden comprenda de manera detallada lo que ordena la ley.
c. Es la misma Ley Estatutaria 1581 de 2012 la que de manera expresa exige unos requisitos para entenderse cumplidas sus disposiciones. Entonces si la investigada no da cumplimiento a lo establecido expresamente en ese cuerpo normativo no puede esta autoridad ignorar esta situación.
   Por ejemplo, en su escrito de reposición la sociedad afirma que: "(…) *la Política de Tratamiento de Datos Personales de WhatsApp proporciona al titular amplia información sobre sus derechos y cómo puede ejercerlos (…)".* No obstante, esta autoridad pudo constatar que dicho documento **no le informa a los titulares todos los derechos establecidos expresamente en la Ley 1581 de 2012 y sus decretos reglamentarios.**

Por tanto, cuando WhatsApp LLC afirma que:

> "*En conclusión, la Política de Tratamiento de Datos Personales de WhatsApp* ***ya incluye garantías y protecciones a los usuarios*** *que son compatibles con las órdenes emitidas por la Resolución y, además, los artículos del Centro de Ayuda contribuyen a brindar una transparencia adicional*". (Destacamos).

Esto no quiere decir que la compañía cumple con **todo lo establecido por el Régimen General de Protección de Datos Personales de la República de Colombia.** Sí es cierto que cuenta con garantías y protecciones a los usuarios, precisamente, aquello fue reconocido en la resolución recurrida. No obstante, el cumplimiento total de las obligaciones y deberes en cabeza de los Responsables del Tratamiento de Datos personales **no es una opción pero sí un deber legal**.

La Organización de las Naciones Unidas (ONU), ha sido enfática en señalar la importancia de "*utilizar al máximo el progreso científico y tecnológico en beneficio del hombre y de neutralizar las actuales consecuencias negativas de algunos logros científicos y tecnológicos, así como las que puedan tener en el futuro*". También, ha destacado que "*los logros científicos y tecnológicos pueden*

entrañar peligro para los derechos civiles y políticos de la persona o del grupo y para la dignidad humana". De esta manera, es necesario alcanzar un punto de **equilibrio entre la innovación, el desarrollo y la protección de los derechos humanos**.

La Red Iberoamericana de Protección de Datos Personales[30] ha reconocido que,

> *"(…) aunque cada día el mundo es más transfronterizo, global e hiperconectado,* ***ello no significa que las normas nacionales sobre tratamiento de datos personales hayan desaparecido o que no sean de obligatorio cumplimiento.*** *Por eso, para que su producto (…) no sea objetado o cuestionado jurídicamente* ***es muy relevante que desde el inicio realice un estudio de riesgos legales de las regulaciones nacionales****.*
>
> *Lo anterior le permitirá definir una estrategia inteligente, para, entre otros, (i) mitigar dichos riesgos; (ii) Ganar y mantener la confianza de los usuarios de las tecnologías (…); (iii) no afectar la buena reputación de su organización y (iv) evitar eventuales investigaciones de las autoridades de protección de datos o de otras entidades*". (Destacamos).

Entonces, es importante identificar en que naciones la organización realiza un tratamiento sobre datos personales, para que así, se pueda diseñar una estrategia de cumplimiento de las normas locales sobre el tratamiento de datos personales. Para terminar, se le recuerda a la sociedad recurrente que la **Resolución Nº 29826 del 19 de mayo del 2021** emitió unas órdenes administrativas y estableció la **manera como deben acreditarse dichas ordenes.**

8. WHATSAPP LLC ESTÁ EN LA OBLIGACIÓN LEGAL DE REGISTRAR LAS BASES DE DATOS PERSONAL QUE TRATA EN EL TERRITORIO NACIONAL EN EL REGISTRO NACIONAL DE BASES DE DATOS

El artículo 25 de la Ley de Protección de Datos establece que: "*El Registro Nacional de Bases de Datos es el directorio público* ***de las bases de datos sujetas a Tratamiento que operan en el país***". (Destacamos). A su vez, el artículo 2.2.2.26.1.2 del Decreto 1074 de 2015 establece que:

> "*Artículo 2.2.2.26.1.2. Ámbito de aplicación. Serán objeto de inscripción en el Registro Nacional de Bases de Datos, las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual sea realizado por los Responsables del tratamiento que reúnan las siguientes características:*
>
> *a) Sociedades y entidades sin ánimo de lucro que tengan activos totales superiores a 100.000 Unidades de Valor Tributario (UVT).*
> b) *Personas jurídicas de naturaleza pública*".

Por su parte, la sociedad recurrente afirma lo siguiente:

> "*Finalmente, como cuestión de fondo, la orden de la SIC se basa en evidencia insuficiente, ya que nunca investigó adecuadamente si los activos de WhatsApp en Colombia superan las 100.000 UVT; de haberlo tenido, la SIC se habría enterado de que WhatsApp no tiene activos en Colombia*".

Luego de aquellas referencias, esta Dirección considera importante destacar lo siguiente:

I. La resolución recurrida le ordenó lo siguiente a la compañía: "*ORDENAR a WhatsApp LLC (en adelante WhatsApp)* ***que respecto de los Datos que recolectan o tratan en el territorio de la República de Colombia sobre personas residentes o domiciliadas en este país****, registren sus Bases de Datos en el Registro Nacional de Bases de Datos (RNBD), administrado por la Superintendencia de Industria y Comercio*". (Destacamos).
II. Como se ha podido comprobar, la sociedad WhatsApp LLC sí realiza un Tratamiento de Datos personales en el territorio de la República de Colombia por medio de web cookies.

[30] La Red Iberoamericana de Protección de Datos (RIPD), surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos. LA RIPD se configura así desde sus orígenes como un foro integrador de los diversos actores, tanto del sector público como privado, que desarrollen iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica, con la finalidad de fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos, así como promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho.

III. El artículo 2.2.2.26.1.2. del Decreto 1074 de 2015 no requiere que los activos de los Responsables estén en Colombia.

Entonces, **WhatsApp LLC está en la obligación de registrar sus bases de datos relativas a los Datos personales que recolecta o trata en el territorio de la República de Colombia** en el Registro Nacional de Bases de Datos (RNBD).

9. DE LA PRESUNTA AFECTACIÓN AL BUEN NOMBRE DE LA COMPAÑÍA WHATSAPP LLC

La sociedad recurrente afirma en su recurso de reposición lo siguiente:

> "*La Resolución impactó el buen nombre, reputación y posición de WhatsApp, lo que ha interferido con su capacidad para cumplir con su objeto social. Como resultado de la conclusión de la Resolución de que WhatsApp trató datos personales en Colombia, WhatsApp ha sido condenado ante el público en general y sus usuarios como una supuesta entidad infractora de la ley*".

Como es sabido, el artículo 165 del Código General del Proceso establece la libertad para acreditar los hechos por cualquier medio útil en los siguientes términos:

> "*Son medios de prueba la declaración de parte, la confesión, el juramento, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios, los informes y* ***cualesquiera otros medios que sean útiles para la formación del convencimiento del juez****.*
>
> *El juez practicará las pruebas no previstas en este código de acuerdo con las disposiciones que regulen medios semejantes o según su prudente juicio, preservando los principios y garantías constitucionales*". (Destacamos).

La jurisprudencia de la Corte Suprema de Justicia[31], por su parte, ha establecido la diferencia entre deberes, obligaciones y cargas procesales, en los siguientes términos:

> "*Son* ***deberes procesales aquellos imperativos establecidos por la ley*** *en orden a la adecuada realización del proceso y que miran, unas veces al Juez (Art. 37 C. de P. C.), otras a las partes y aun a los terceros (Art. 71 ib.), y su incumplimiento se sanciona en forma diferente según quien sea la persona llamada a su observancia y la clase de deber omitido (arts. 39, 72 y 73 ibídem y Decreto 250 de 1970 y 196 de 1971). Se caracterizan porque emanan, precisamente, de las normas procesales, que son de derecho público, y, por lo tanto, de imperativo cumplimiento en términos del artículo 6° del Código.*
>
> ***Las obligaciones procesales son, en cambio, aquellas prestaciones de contenido patrimonial impuestas a las partes con ocasión del proceso****, como las surgidas de la condena en costas que, según lo explica Couture, obedecen al concepto de responsabilidad procesal derivada del abuso del derecho de acción o del derecho de defensa. "El daño que se cause con ese abuso, dice, genera una obligación de reparación, que se hace efectiva mediante la condenación en costas". ("Fundamentos del Derecho Procesal Civil", número 130).*
>
> *Finalmente,* ***las cargas procesales son aquellas situaciones instituidas por la ley que comportan o demandan una conducta de realización facultativa, normalmente establecida en interés del propio sujeto y cuya omisión trae aparejadas para él consecuencias desfavorables****, como la preclusión de una oportunidad o un derecho procesal e inclusive hasta la pérdida del derecho sustancial debatido en el proceso.*
>
> *Como se ve, las cargas procesales se caracterizan porque el sujeto a quien se las impone la ley conserva la facultad de cumplirlas o no, sin que el Juez o persona alguna pueda compelerlo coercitivamente a ello, todo lo contrario de lo que sucede con las obligaciones; de no, tal omisión le puede acarrear consecuencias desfavorables. Así, por ejemplo probar los supuestos de hecho para no recibir una sentencia adversa*". (Subrayado fuera del texto).

[31] Sala de Casación Civil, M.P. Dr. Horacio Montoya Gil, auto del 17 de septiembre de 1985, que resolvió una reposición, Gaceta Judicial TOMO CLXXX – No. 2419, Bogotá, Colombia, Año de 1985, pág. 427.

Con esto en mente, la sociedad recurrente tenía la **carga procesal** de **probarle** a esta Superintendencia que la resolución recurrida impactó el buen nombre, reputación y posición de WhatsApp en el territorio de la República de Colombia. Sin embargo, un estudio completo e integro del expediente da cuenta como la sociedad investigada **no acompañó sus afirmaciones con las pruebas idóneas y útiles que demostrarán dicha situación.** En otras palabras, no basta la mera afirmación de las recurrentes para acreditar debidamente un hecho. Es necesario, presentar evidencia para corroborar esas aseveraciones.

10. WHATSAPP NO ESTÁ OBLIGADO A CONTAR CON UNA DIRECCIÓN DE CORREO ELECTRÓNICO PARA NOTIFICACIONES ELECTRÓNICAS

La sociedad recurrente acierta cuando afirma en su recurso de reposición lo siguiente: *"El artículo 4 de la Resolución exhorta a WhatsApp a proporcionar a la SIC una dirección de correo electrónico en la que pueda recibir comunicaciones o notificaciones de actos administrativos*".

De acuerdo con la Real Academia Española (en adelante RAE) la palabra "*exhortar" significa "Incitar a alguien con palabras a que haga o deje de hacer algo*"[32]. Por tanto, **en ningún momento esta Dirección estaba obligando o forzando a la sociedad WhatsApp a proporcionar una dirección de correo electrónico.**

La invitación a que dicha sociedad proporcionara una dirección de correo electrónico tiene como objetivo mejorar la comunicación entre la entidad y el Responsable del Tratamiento. Además, sería una herramienta útil para que WhatsApp LLC pueda "*presentar a la SIC el ámbito y alcance de sus compromisos, de sus políticas de tratamiento y las medidas implementadas para asegurar la transparencia de sus prácticas y los derechos de los usuarios como titulares de datos personales*" como lo afirma en su recurso.

11. RESPONSABILIDAD DEMOSTRADA *(ACCOUNTABILITY)* 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*"[33].

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

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

El artículo 26[34] *-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

---

[32] https://dle.rae.es/exhortar

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

[34] 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"*

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]."[35]

Es de resaltar que la Corte Constitucional mediante la Sentencia C-32 de 2021 reconoció la existencia de la responsabilidad demostrada 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 (sic). 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. Esto de manera proporcional a: (i) la naturaleza jurídica del responsable y, cuando sea el caso, su tamaño empresarial; (ii) la naturaleza de los datos personales objeto de tratamiento; (iii) el tipo de tratamiento; y (iv) los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares del dato personal. Con este fin, los responsables deben informar a la SIC acerca de los procedimientos usados para el tratamiento de datos. A esta medida se suma lo previsto en el artículo 27 ejusdem, que estipula la obligación del responsable de establecer políticas internas que garanticen: (i) la existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable; (ii) la adopción de mecanismos internos para poner en práctica dichas políticas; y (iii) la previsión de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, respecto de cualquier aspecto del tratamiento de datos personales.*
>
> *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"*[36]. (Destacamos).

Como se observa, la Corte Constitucional pone de presente en la obligación de demostrar que se han adoptado medidas para cumplir la regulación de Datos personales.

El Principio de Responsabilidad Demostrada –*accountability*- demanda implementar acciones de diversa naturaleza[37] 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

---

[35] 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".*

[36] Cfr. Corte Constitucional, sentencia C-032 del 18 de febrero de 2021. M.P. Dra Gloria Stella Ortiz. El texto de la sentencia puede consultarse en: https://www.corteconstitucional.gov.co/relatoria/2021/C-032-21.htm

[37] 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.

de los Datos Personales. El éxito del mismo, dependerá del compromiso real y ético 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****"*[38]. (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.

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

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

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

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

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

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

---

[38] 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.

Ahora, según el artículo 22 de la Ley 222 de 1995[39] la expresión administradores comprende al "*representante legal, el liquidador, el factor, los miembros de juntas o consejos directivos y quienes de acuerdo con los estatutos ejerzan o detenten esas funciones*". Cualquiera de ellos tiene la obligación legal de garantizar los derechos de los Titulares de los Datos y de cumplir la Ley 1581 de 2012 y cualquier otra norma concordante. Por esto, el numeral segundo del artículo 23 de la Ley 222 de 1995 determina que los administradores deben "*obrar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios*", y además, en el ejercicio de sus funciones deben "*velar por* ***el estricto cumplimiento de las disposiciones legales o estatutarias***". (Énfasis añadido).

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

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

El artículo 24[40] de la Ley 222 de 1995, presume la culpa del administrador "*en los casos de incumplimiento o extralimitación de sus funciones, violación de la ley o de los estatutos*". Esta presunción de responsabilidad, exige que los administradores estén en capacidad de probar que han obrado con lealtad y la diligencia de un experto. Es decir, como un "*buen hombre de negocios*", tal y como lo señala su artículo 23.

Adicionalmente, no debe perderse de vista que los administradores responden "*solidaria e ilimitadamente de los perjuicios que por dolo o culpa ocasionen a la sociedad, a los socios o a terceros*"[41]. Las disposiciones referidas, prevén unos elementos de juicio ciertos, i) el alto nivel de responsabilidad jurídica y económica en cabeza de los administradores, y ii) el enorme profesionalismo y diligencia que debe rodear su gestión en el Tratamiento de Datos personales.

CONCLUSIONES

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

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

- WhatsApp LLC mediante mecanismos electrónicos recolecta Datos personales en el territorio de la República de Colombia. Por ende, ese Tratamiento de Datos personales está sujeto a la

---

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

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

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

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

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

- WHATSAPP LLC emplea diversas tecnologías para recolectar datos personales en el territorio de la República de Colombia, entre las que se incluyen las web cookies.

- Esta autoridad en ningún momento obligó o forzó a la sociedad WhatsApp a proporcionar una dirección de correo electrónico.

- WhatsApp LLC está en la obligación de registrar sus bases de datos relativas a los Datos personales que recolecta o trata en el territorio de la República de Colombia en el Registro Nacional de Bases de Datos (RNBD).

- La Superintendencia de Industria y Comerció notificó el acto administrativo recurrido de acuerdo con la legislación colombiana. Respetando, en todo momento, el derecho fundamental al debido proceso en cabeza de la sociedad WhatsApp LLC.

- La regulación colombiana sobre Tratamiento de datos impone al Responsable del Tratamiento el deber demostrar que ha adoptado medidas efectivas para cumplir la ley (Deber de Responsabilidad demostrada).

- WhatsApp LLC no logró probar como la resolución recurrida impactó el buen nombre, reputación y posición de WhatsApp en el mercado colombiano. No basta la mera afirmación de las recurrentes para acreditar debidamente un hecho.

- No es sensato que quien recolecte y trate datos en el territorio de la República de Colombia - *sin estar domiciliado o residir en el mismo* - acuda a argumentos clásicos de territorialidad no solo para para evadir sus responsabilidades legales frentes a las autoridades y los titulares de los datos, sino para desconocer el ámbito de aplicación de la citada ley.
- Entonces, es importante identificar en que naciones la organización realiza un tratamiento sobre datos personales, para que así, se pueda diseñar una estrategia de cumplimiento de las normas locales sobre el tratamiento de datos personales.

De esta forma y de acuerdo con lo dispuesto por el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, esta Dirección confirma la **Resolución Nº 29826 del 19 de mayo del 2021**.

En mérito de lo expuesto, este Despacho,

RESUELVE

ARTÍCULO PRIMERO. CONFIRMAR la **Resolución Nº 29826 del 19 de mayo del 2021** de conformidad con lo expuesto en la parte motiva del presente acto administrativo.

ARTÍCULO SEGUNDO. Conceder el recurso subsidiario de apelación interpuesto en contra de la **Resolución Nº 29826 del 19 de mayo del 2021**, 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 WhatsApp LLC.

ARTÍCULO CUARTO: La Superintendencia de Industria y Comercio se permite recordar que los canales habilitados para que los investigados ejerzan sus derechos, den respuesta a requerimientos, interpongan recursos, entre otros, son:

- Correo Superindustria: contactenos@sic.gov.co
- Sede Principal: Carrera 13 No. 27 - 00, Pisos 1 y 3 en la Ciudad de Bogotá, de lunes a viernes de 8:00 a.m. a 4:30 p.m.

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., 08 FEBRERO DE 2022

El Director de Investigación de Protección de Datos Personales,

CARLOS ENRIQUE SALAZAR MUÑOZ

Firmado digitalmente por CARLOS ENRIQUE SALAZAR MUÑOZ
Fecha: 2022.02.08 10:51:42 -05'00'

CARLOS ENRIQUE SALAZAR MUÑOZ

ALC

NOTIFICACIÓN:

Sociedad (1):	**WhatsApp LLC**
Identificación:	N/A[42]
Correo electrónico:	N/A[43]
Dirección:	1601 Willow Road Menlo Park, California 94025 Estados Unidos de América

[42] No se cuenta con la identificación
[43] No se cuenta con la identificación