

REPÚBLICA DE COLOMBIA



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

RESOLUCIÓN NÚMERO 74924 DE 2021

(Noviembre 19 de 2021)

Por la cual se resuelve un recurso de apelación

Radicado No. 17-154376

VERSIÓN PÚBLICA

EL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES

En ejercicio de sus facultades legales, en especial las conferidas por los artículos 19 y 21 de la Ley 1581 de 2012 y el numeral 7 del artículo 16 del Decreto 4886 de 2011 y,

CONSIDERANDO:

PRIMERO: Que mediante oficio 17-154376-00 del 6 de junio de 2017, el señor [REDACTED], presentó ante esta superintendencia queja en contra de **NOVOCLICK – TUCONSULTA COLOMBIA S.A.S.** (en adelante **TUCONSULTA**) al considerar vulnerado su derecho de *habeas data*.

SEGUNDO: Que mediante Resolución No. 58059 del 29 de octubre de 2019 la Dirección de Investigación de Protección de Datos Personales resolvió iniciar una investigación administrativa con el fin de establecer si **TUCONSULTA**, infringió las normas sobre protección de datos personales consagradas en: **(i)** literal b) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal c) del artículo 4 y el artículo 9 de la misma ley, como también con el artículo 2.2.2.25.2. del Decreto Único Reglamentario 1074 de 2015; y, **(ii)** literal c) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal b) del artículo 4 y el artículo 12 de la misma Ley.

TERCERO: Que una vez agotada la etapa probatoria y efectuado el análisis del escrito de descargos¹ y de los diferentes medios probatorios allegados oportunamente al expediente, la Dirección de Investigación de Protección de Datos Personales resolvió, mediante la Resolución No. 41383 del 2 de julio de 2021, lo siguiente:

“ARTÍCULO PRIMERO: IMPONER una sanción pecuniaria a la sociedad **TU CONSULTA COLOMBIA S.A.S.**, identificada con NIT. 900.318.063-5, de **TRES MILLONES DOSCIENTOS SESENTA Y SIETE MIL SETECIENTOS VEINTE PESOS M/CTE (\$3.267.720)**, equivalente a **NOVENTA (90) UNIDADES DE VALOR TRIBUTARIO – UVT**, por la violación de lo dispuesto en el literal c) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal b) del artículo 4 y el artículo 12 de la misma ley.

ARTÍCULO SEGUNDO: ORDENAR a la sociedad **TU CONSULTA COLOMBIA S.A.S.**, identificada con NIT. 900.318.063-5, que dentro del término de **DOS (2) MESES** siguientes a la ejecutoria de la presente decisión, de cumplimiento a las siguientes instrucciones:

- La sociedad **TU CONSULTA COLOMBIA S.A.S.**, identificada con NIT 900.318.063-5, deberá retirar la selección por defecto en los diferentes checkbox habilitados en los formularios de inscripción que tiene dispuestos y que llegue a implementar en su página web, así como en los diferentes medios electrónicos que disponga para la recolección de datos, de acuerdo con lo dispuesto en la Ley 1581 de 2012 y el Decreto Único Reglamentario 1074 de 2015.
- La sociedad **TU CONSULTA COLOMBIA S.A.S.**, identificada con NIT 900.318.063-5, deberá en los formularios en los que pregunta *¿cuánto invierte en publicidad al año?* Informar la Política de Tratamiento de Datos Personales y habilitar un mecanismo para que el Titular decida si acepta que su información se trate bajo lo dispuesto en ella.
- La sociedad **TU CONSULTA COLOMBIA S.A.S.**, identificada con NIT. 900.318.063-5, deberá implementar los mecanismos necesarios para garantizar que el Titular de la información consulte la Política de Protección de Datos Personales y sea informado de lo previsto en el artículo 12 de la Ley 1581 de 2012 cuando accede a los formularios de inscripción que tiene dispuestos y que llegue a implementar en su página web, así como en los diferentes medios electrónicos que disponga para la recolección de datos”.

¹ Actuación radicada en el sistema de trámites de la entidad bajo el número 17-154376-26 del 4 de diciembre de 2019.

CUARTO: Que en el término legal establecido para el efecto², mediante escrito 17-154376-59 del 30 de julio de 2021, el Representante Legal de **TUCONSULTA**, (en adelante el **RECURRENTE**) interpuso el recurso de reposición y en subsidio de apelación contra la Resolución No. 41383 del 2 de julio de 2021, en los siguientes términos:

"FUNDAMENTOS DE DERECHO DEL RECURSO:

Bajo la circunstancia que atañe la motivación de este recurso, este honorable despacho encuentra que mi empresa, esto es, la Sociedad TuConsulta Colombia S.A.S, habría vulnerado el Régimen General de Protección (sic) de Datos Personales, por la circunstancia de no contar con Autorización conforme a las disposiciones legales y reglamentarias, para tratar los datos personales del denunciante desde el año 2017.

Como pasaremos a exponer y fue suficientemente explicado en el curso de la investigación administrativa que sirve de marco de referencia para la imposición de la sanción, la empresa si contaba con distintos mecanismos tanto para divulgar la Política de tratamiento de datos y mecanismos técnicos para recoger las autorizaciones con la incorporación de checkbox como forma automatizada de que el titular manifestara su consentimiento.

AUTORIZACION PARA EL TRATAMIENTO DE DATOS PERSONALES EN LOS FOMULARIOS WEB DE NOVOCCLICK

Como se ha expresado a lo largo de las etapas procesales surtidas en el presente caso, tenemos implementado varios mecanismos para la recolección de los datos de nuestros visitantes y usuarios al sitio web de nuestra empresa y en la mayoría existía desde el momento en el que inicio esta investigación (Año 2017) los mecanismos de checkbox y elementos como el Recaptcha que permite garantizar que los mismos no sean diligenciados por robots u otros mecanismos similares.

La entidad en su afán de presentarnos como vulneradores de la norma, decide concentrarse en el único formulario (Que además solo funcionaba como trigger para el inicio frente a consultas) que no poseía el mecanismo de checkbox para la autorización. Esto lo advertimos a la entidad tanto en nuestros descargos como en el curso de la investigación, pero no fue tenido en cuenta. Si hoy se revisa el sitio web, todos los mecanismos señalados en la Resolución y que hoy son objeto de una orden administrativa por supuesto los tenemos implementados.

Si bien, la SIC insiste en que la autorización es el mecanismo fundamental para legitimar el tratamiento de los datos, no debe perderse de vista, que fenómenos como el comercio electrónico y la transformación digital han impuesto nuevas realidades para la captura de información sin que esta, per se, este precedida de un conocimiento siquiera del titular de los datos. Y a pesar que a ojos de la entidad esto suponga un reproche, es la forma, en que están configuradas tecnologías actuales. Así por ejemplo, la conexión a sitios web desde dispositivos, tienen como precedente, que se capturen datos y otros tipos de información como lugar de conexión, navegadores, fecha y hora por supuesto, de quien accede a un sitio web. Con la intención de reforzar lo antes expuesto, traigo a colación lo estipulado por el Reglamento Europeo de Protección (sic) de Datos, que sobre el particular señaló

"Artículo 6: Licitud del tratamiento:

El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

... el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos"

Así mismo el Art. 7 del RGPD. Condiciones para el consentimiento

...Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales."

La principal novedad que se introduce en el RGPD con respecto a la normativa es que el consentimiento debe de consistir en una declaración afirmativa o una clara acción afirmativa para la prestación del mismo, no admitiéndose por tanto el consentimiento tácito.

*De esta manera, el consentimiento debe de ser claro de tal forma que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado. Expresamente se indica en el **considerando 32** la posibilidad de utilizar casillas para la obtención del mismo, estableciendo que la casilla **pre marcada o la inacción no constituye** una forma de prestar el consentimiento. Igualmente, también se establece en dicho considerando que cuando existan varios fines para el tratamiento se deberá recabar el consentimiento para todos ellos.*

... Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales.

Concluimos entonces para nuestro caso de marras, que si bien la Entidad ha optado por indicar que las casillas premarcadas no constituyen una forma valida del consentimiento; no es menos cierto que, esta situación vino a ser incorporada inicialmente por el RGPD o Reglamento General de Protección de Datos en 2016, en vigor desde Mayo de 2018 y sus postulados fueron expresados por la SIC en Conceptos recientes como una medida de buena practica que en todo caso, no fue antes de la ocurrencia de los hechos que originaron esta actuación

² Conforme a constancia suscrita por el Coordinador del Grupo de Notificaciones y Certificaciones de esta Superintendencia, radicada en el sistema de trámites bajo el número 17-154376-58 del 21 de julio de 2020, la Resolución No. 41383 del 2 de julio de 2021, fue notificada por aviso a TU CONSULTA el día 15 de julio de 2021.

administrativa. Así las cosas, era imposible que para 2017 nuestros mecanismos reflejaran la buena práctica de no estar PREMARCADAS las casillas en el checkbox de autorización.

Dado lo anteriormente expuesto es claro para la empresa que, contrario a las conclusiones esbozadas por la entidad, los mecanismos que utilizábamos para la época de apertura de investigación y denuncia del titular de los datos, eran válidos y no merecían reproche alguno.

Por otra parte, en la Resolución y en el curso de la investigación se concluye válidamente que los datos que fueron objeto de tratamiento se consideran datos de naturaleza pública, ajenos a las actividades comerciales que su titular ejecutaba, pero a renglón seguido de tal conclusión, reprocha la entidad el cumplimiento del resto de requisitos respecto del régimen de protección de datos. Esta situación que merece un análisis mucho más profundo a nivel jurídico, que como Gerente no logro realizar, me parece que no es acorde y viola el Principio de congruencia que debe existir entre los cargos objeto de investigación y los resultados del procedimiento sancionatorio; ya que se nos investiga por una cosa, pero terminamos siendo sancionados por otra. Si la investigación se dirigió a establecer si contábamos con la autorización del titular de los datos y se concluyó que, por la naturaleza de los datos, la misma NO ERA NECESARIA, lo lógico es que se archivara la investigación o concluyera con las Ordenes administrativas.

Por lo anterior, sea esta una nueva oportunidad para que la entidad REVOQUE su decisión y ordene el archivo de la investigación o mantenga las Ordenes administrativas, que dicho sea de paso estamos muy dispuestos a cumplir y demostrar a la entidad en el plazo otorgado.

FALTA DE APLICACION DEL PRINCIPIO DE RAZONABILIDAD Y PROPORCIONALIDAD EN LA IMPOSICION DE SANCIONES.

Solicitamos a la entidad como segunda Petición, se revise el monto de la sanción. Si bien la misma, a cualquiera puede parecerle baja, no es menos cierto que en el momento actual de nuestra empresa es MUY ALTA. Con el objeto de que la misma sea rebajada, en caso de no accederse a su revocatoria total, estoy adjuntando con este recurso la última certificación de ingresos de nuestra empresa correspondiente a la vigencia fiscal de 2020 y lo corrido del 2021 donde se puede evidenciar el grave estado de nuestra posición económica, la cual resultaría más perjudicada con el pago de esta sanción, casi que nos llevaría a la Quiebra.

A este respecto me permito traer algunas consideraciones:

En aras de respetar el principio de legalidad, **en los casos de discrecionalidad**, en el momento previo a la **decisión de sancionar la autoridad deberá determinar, en primer lugar, la fuente de su discrecionalidad** o, lo que es lo mismo, dónde se ubica esta facultad decisoria: en la **escogencia de la sanción a imponer** o en la tasación de la sanción a imponer. Esto, debido a que aun cuando en uno y otro caso debe haber un marco legal que encuadre dicha discrecionalidad administrativa (que hace que se deba hablar siempre de la convergencia en este campo del principio de legalidad con el de proporcionalidad), también existen diferencias notables entre un supuesto y otro.

Si la discrecionalidad se ubica en la elección de la sanción a imponer, **en virtud del principio de legalidad**, el operador sancionatorio **deberá respetar las opciones que le ofrece la norma legal** (multa, suspensión, caducidad, etc.), que **constituyen un límite a su poder de decisión**. En todo caso la Ley ofrece solo un repertorio de posibilidades, por lo cual **al definir qué medida adoptar en concreto debe obrar con apego a las exigencias de los principios de ponderación y proporcionalidad, y tener en cuenta que su decisión se debe conformar a lo previsto por el artículo 44 del CPACA**, de acuerdo con el cual "[e]n la medida en que el contenido de una decisión de carácter general o particular sea discrecional, debe ser adecuada a los fines de la norma que la autoriza y proporcional a los hechos que le sirven de causa".

Sea cual sea la decisión que adopte, la no infracción de la garantía del debido proceso exige la **plena motivación de la decisión**. Por ende, debe quedar manifiesto que **la severidad de la sanción es función de la gravedad de la conducta reprochada**, de suerte que a mayor gravedad esta última mayor severidad de la primera.

Si la discrecionalidad se ubica **en la graduación de la sanción**, la autoridad debe **determinar si la norma especial que rige su competencia prevé algunos criterios de graduación** de la sanción. De no estar contempladas deberá analizar los **criterios generales que establece el CPACA**. De no resultar aplicable ninguno de ellos, tendrá mayor margen de acción, pero deberá tomar una decisión teniendo en cuenta lo previsto por el artículo 44 del CPACA ya citado, so pena de infringir los principios de ponderación y proporcionalidad".

Por lo anterior, solicitamos en forma subsidiaria a la primera pretensión, que, en caso de no considerar la revocación absoluta de la sanción pecuniaria, se establezca una **REDUCCION SUSTANCIAL o ELIMINACION** de la sanción con ocasión de los motivos expuestos con este recurso.

PETICIONES:

PRIMERO: Se revoque en su totalidad la Sanción Económica contenida en la Resolución 41383 del 02 de Julio de 2021, por las razones y motivos anteriormente señalados.

SEGUNDO: En forma subsidiaria en caso de que la primera pretensión no sea acogida solicitamos se modifique el artículo primero de la Resolución N° 41383, específicamente en el sentido de disponer LA DISMINUCIÓN DE LA MULTA o ELIMINACIÓN impuesta a TuConsulta Colombia S.A.S, de conformidad con los criterios de razonabilidad y proporcionalidad relativos a la dosimetría de la sanción.

QUINTO: Que mediante Resolución No. 55363 del 30 de agosto de 2021, el Director de Investigación de Protección de Datos Personales resolvió el recurso de reposición interpuesto, confirmando la Resolución No. 41383 del 2 de julio de 2021, y concediendo el recurso de apelación presentado de manera subsidiaria por el **RECURRENTE**.

SEXTO: Que de conformidad con lo establecido en el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, este Despacho procede a resolver el recurso de apelación interpuesto contra la Resolución No. 41383 del 2 de julio de 2021, de conformidad con las siguientes,

CONSIDERACIONES DEL DESPACHO:

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

El artículo 16 del Decreto 4886 de 26 de diciembre de 2011³ establece las funciones del Superintendente Delegado para la Protección de Datos Personales, entre las cuales se destacan las siguientes:

"(...)

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

(...)"

2. DE LAS PRUEBAS ALLEGADAS A LA PRESENTE ACTUACIÓN ADMINISTRATIVA.

Previo a resolver el recurso de apelación interpuesto, este Despacho hará un breve pronunciamiento respecto de las pruebas que fueron allegadas a la presente actuación administrativa.

2.1. Acta de Preservación de Páginas Web No. 118-18 del 24 de mayo de 2018, mediante la cual, respecto del sitio web www.novoclick.com se informó lo siguiente:

Datos personales observados: se observa un formulario que recolecta los siguientes datos personales: nombre, e-mail y teléfono

Consulta datos de titulares: No es posible consultar datos de titulares desde el referido sitio web.

Se solicita autorización al titular para el tratamiento de sus datos personales:

De acuerdo al requerimiento, se realiza una revisión del sitio web <http://www.novoclick.com> observando la existencia de un chat de ayuda (¿necesita ayuda?) el cual en la parte inferior se ubica un checkbox activado por defecto el cual da por aprobada la política de privacidad y de tratamiento de datos.

La política de Tratamiento se encuentra publicada en la página:

De acuerdo al requerimiento, se realiza revisión del sitio web <http://www.novoclick.com>, encontrando que se puede acceder a la política de privacidad y de tratamiento de datos haciendo click sobre el texto ubicado en la parte inferior de la ventana del chat ¿necesita ayuda? Abriendo una nueva ventana del navegador con la dirección <http://www.novoclick.net/politicas-de-privacidad-2013>.

Datos de menores de edad: no se observa recolección de datos de menores de edad en el sitio web <http://www.novoclick.com>.

Canales de atención PQRS: no se evidencia la existencia de canales de atención PQRS.

Si el sitio web cuenta con las condiciones de seguridad necesarias para impedir la alternación, pérdida, consulta, uso o acceso no autorizado.

De acuerdo al requerimiento, se realiza una revisión de los sitio web <http://www.novoclick.com>, las condiciones básicas de seguridad se detallan a continuación.

³ Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones.

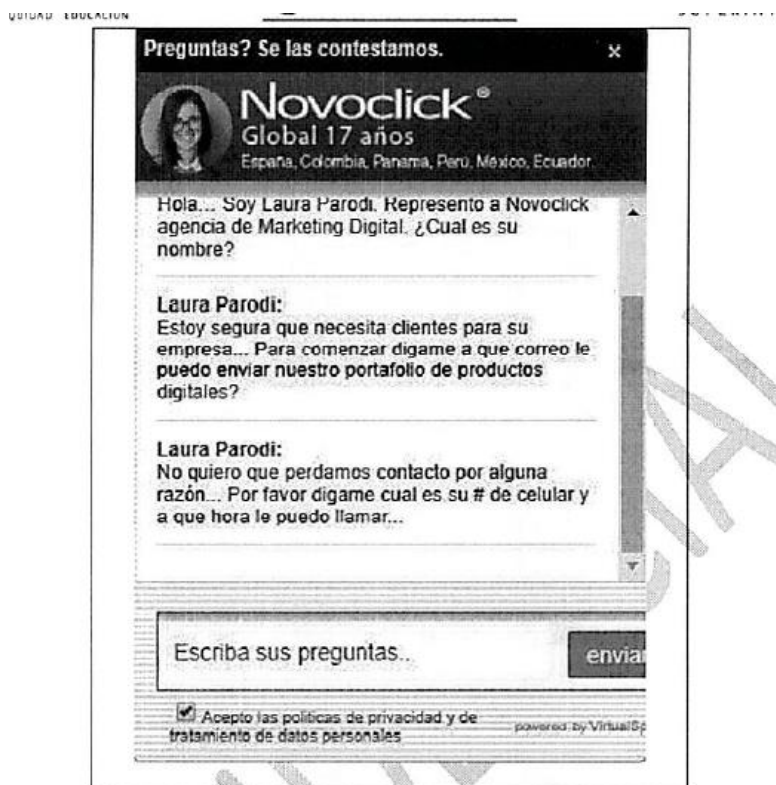


Imagen 8. Chat de contacto, obtenida con impresión por pantalla la Aplicación de Microsoft Windows

Como se observa, existe un signo de aceptación de políticas de privacidad y tratamiento de datos personales pero ello no significa que el titular del dato esté autorizando la recolección y uso de la información. La autorización es el "*consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales*"⁴, mientras que la política de tratamiento de datos es un documento informativo que debe contener lo que ordena el artículo 13 del decreto 1377 de 2013.

2.2. Mediante Resolución No. 9541 del 3 de marzo de 2020, la Dirección de Investigación de Protección de Datos Personales, decretó de oficio las siguientes pruebas:

- La sociedad **TUCONSULTA COLOMBIA S.A.S.**, deberá aportar prueba técnica mediante la cual se acredite que para la fecha de recolección de los datos del titular, contaba con el mecanismo "Checkbox", mediante el cual los titulares conocen y aceptan las Políticas de Privacidad antes de autorizar el uso de sus datos personales y los medios a través de los cuales son informados sobre la finalidad del tratamiento de su información.
- La sociedad **TUCONSULTA COLOMBIA S.A.S.**, deberá aportar prueba técnica que demuestre que los datos del titular son de naturaleza pública y la forma como fueron recolectados.

2.3. Oficio No. 17-154376-33 de fecha 14 de julio de 2020, mediante el cual el Representante Legal de **TUCONSULTA** allega las pruebas requeridas por la Dirección relacionadas en el numeral anterior.

2.4. Acta de Análisis Técnico de Expedientes de la Delegatura de Protección de Datos Personales de fecha 12 de agosto de 2020, mediante la cual se realiza una verificación técnica a la información enviada por parte de **TUCONSULTA**, relacionada en el numeral anterior, y de la cual se extraen las siguientes imágenes y conclusiones:

Numeral 2. "Prueba Técnica Verificación CHECKBOX EN CADA PORTAL DE NOVOCLICK la sociedad hace referencia a los siguientes formularios: FORMULARIO INSCRIPCIÓN NOVOCLICKCANALES; FORMULARIO INSCRIPCIÓN NOVOCLICKNAVIDAD; FORMULARIO INSCRIPCIÓN CONSIGACLIENESPASUEMPRESA; FORMULARIO INSCRIPCIÓN NOVOLLENODECLIENES; FORMULARIO INSCRIPCIÓN NOVOPAN; FORMULARIO INSCRIPCIÓN NOVOCLICKPANAMA2015; FORMULARIO INSCRIPCIÓN NOVOCLICKNAVIDAD

Se procedió a abrir cada uno de los enlaces suministrados como respuesta, encontrando que los formularios reportados contienen un mecanismo de aceptación de políticas de privacidad y de tratamiento de datos personales consistente en un checkbox, se evidencia que este se encuentra activado por defecto como se aprecia en las siguientes imágenes:

⁴ Cfr. Literal a) del artículo 3 de la Ley Estatutaria 1581 de 2012

FORMULARIO INSCRIPCIÓN NOVOCLICKANALES
<https://novoclick.com.pa/panel/AC0467NOVOCLICKANALES/novoclick/>



Imagen 2. Enlace aportado, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes

FORMULARIO INSCRIPCIÓN NOVOCLICKNAVIDAD
<https://novoclick.com.pa/panel/EB0065NOVOCLICKNAVIDAD/novoclick/>

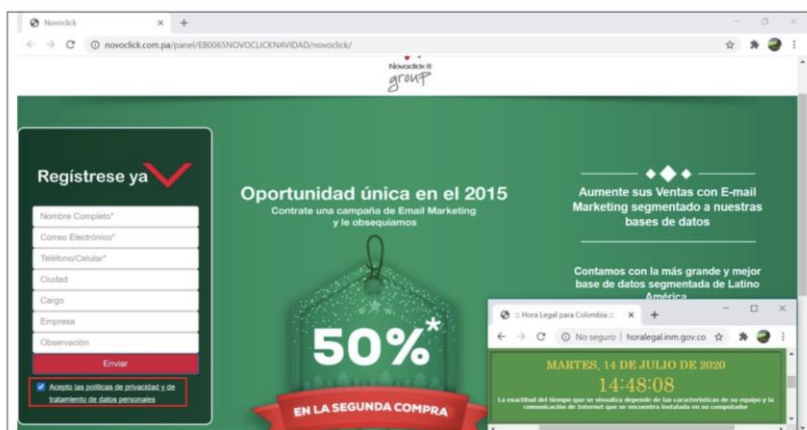


Imagen 3. Enlace aportado, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes

FORMULARIO INSCRIPCIÓN CONSIGACLIENTESPARASUEMPREASA
<https://novoclick.com.pa/panel/EB25CONSIGACLIENTESPARASUEMPREASA/novoclick/>

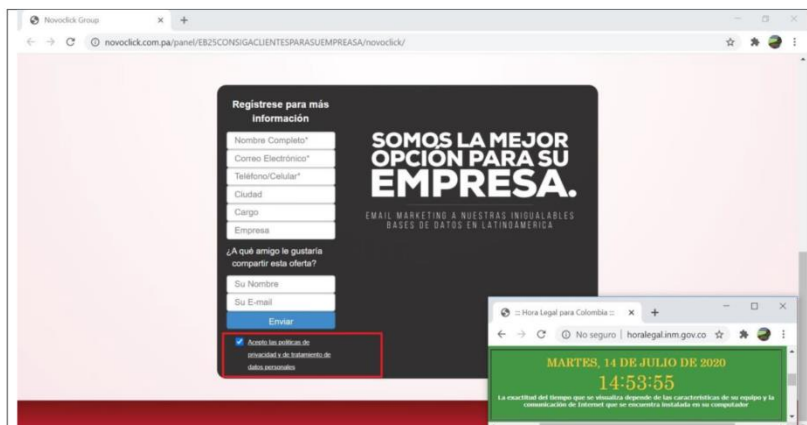


Imagen 4. Enlace aportado, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes

FORMULARIO INSCRIPCIÓN NOVOPAN
<https://novoclick.com.pa/panel/OB0075NOVOPANAMA/novoclick/>

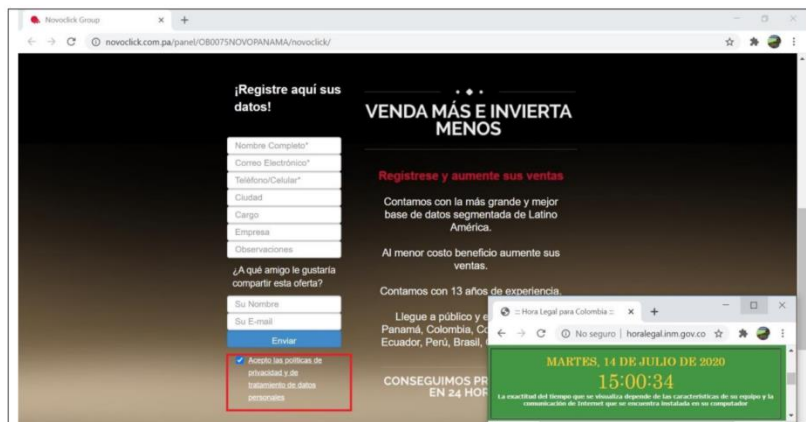


Imagen 5. Enlace aportado, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes

FORMULARIO INSCRIPCIÓN NOVOCLICKPANAMA2015
<https://novoclick.com.pa/panel/OB0056NOVOCLICKPANAMA2015/novoclick/>

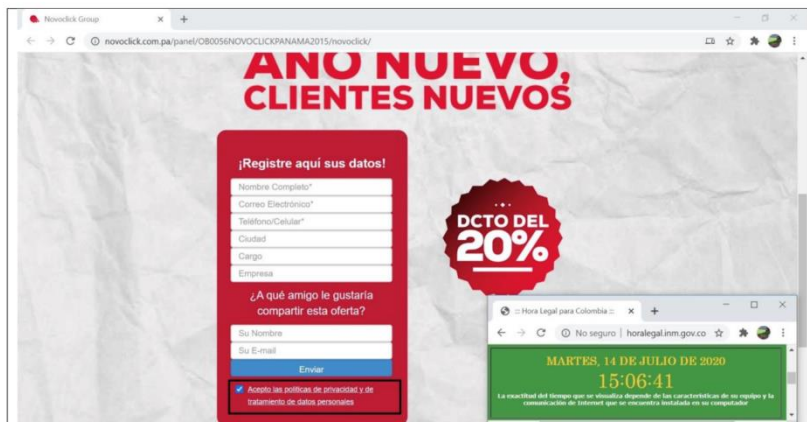


Imagen 6. Enlace aportado, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes

FORMULARIO INSCRIPCIÓN NOVOCLICKNAVIDAD
<https://novoclick.com.pa/panel/AC0015NOVOCLICKNAVIDAD/novoclick/>

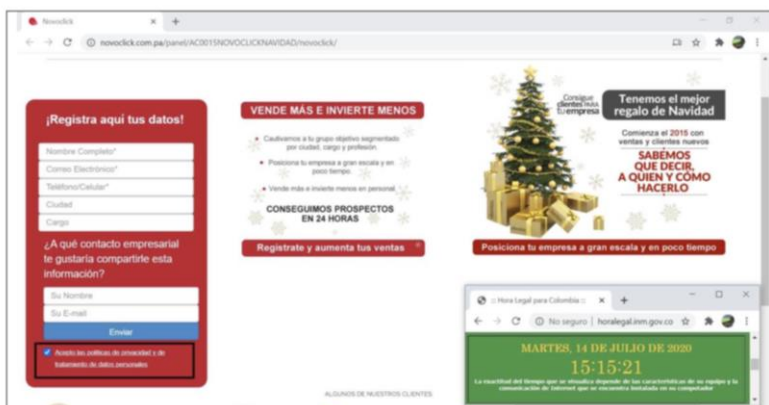


Imagen 7. Enlace aportado, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes

CONCLUSIONES

Una vez analizada la información disponible, se realizan las siguientes conclusiones, las cuales deberán ser evaluadas jurídicamente.

El día el día seis (6) del mes de junio de dos mil dieciocho (2018) se realizó la revisión del sitio web <http://www.novoclick.com>, con el fin de preservar las pruebas que puedan llegar a ser indicios de prácticas en contra del régimen de Protección de Datos Personales por parte de dicho sitio web.

Dentro del acta de preservación se dejó como observación lo siguiente:

Se observa en la página <http://www.novoclick.com/contacto/> un formulario de registro, en el cual se recolectan los siguientes datos personales: nombres y apellidos, correo electrónico y teléfono, el cual no tiene ningún mecanismo de aceptación de tratamiento de datos personales.

Como prueba de lo anterior se anexa captura de pantalla tomada de la copia del referido sitio web, la cual hace parte del expediente con radicado 17-154376:

Imagen 4. Formulario de registro, obtenida con impresión por pantalla la Aplicación de Microsoft Windows Recortes

Respecto a los enlaces contenidos en el numeral 1 de la respuesta, no es posible establecer la fecha en la que los sitios web fueron publicados o modificados.

Los formularios contenidos en el numeral 2 de la respuesta contienen un mecanismo de aceptación de políticas de privacidad y de tratamiento de datos personales consistente en un checkbox, se evidencia que este se encuentra activado por defecto.

3. DEL DEBER DE INFORMAR AL TITULAR SOBRE LA FINALIDAD DE LA RECOLECCIÓN DE DATOS PERSONALES

Indicó el **RECURRENTE** lo siguiente:

"Por otra parte, en la Resolución y en el curso de la investigación se concluye válidamente que los datos que fueron objeto de tratamiento se consideran datos de naturaleza pública, amen de las actividades comerciales que su titular ejecutaba, pero a renglón seguido de tal conclusión, reprocha la entidad el cumplimiento del resto de requisitos respecto del régimen de protección de datos. Esta situación que merece un análisis mucho más profundo a nivel jurídico, que como Gerente no logro realizar, me parece que no es acorde y viola el Principio de congruencia que debe existir entre los cargos objeto de investigación y los resultados del procedimiento sancionatorio; ya que se nos investiga por una cosa, pero terminamos siendo sancionados por otra. Si la investigación se dirigió a establecer si contábamos con la autorización del titular de los datos y se concluyó que, por la naturaleza de los datos, la misma NO ERA NECESARIA, lo lógico es que se archivara la investigación o concluyera con las Ordenes administrativas. (negrilla fuera de texto.)"

De conformidad con lo establecido en la Resolución No. 58059 del 29 de octubre de 2019, le fueron formulados cargos a **TUCONSULTA** por la presunta vulneración de **(i)** literal b) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal c) del artículo 4 y el artículo 9 de la misma ley, como también con el artículo 2.2.2.25.2. del Decreto Único Reglamentario 1074 de 2015; y, **(ii)** literal c) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal b) del artículo 4 y el artículo 12 de la misma Ley.

Respecto del primer cargo formulado, la Dirección resolvió no sancionar a **TUCONSULTA**, en la medida que los datos proporcionados por el quejoso eran de carácter público, y de conformidad con lo establecido en el artículo 10 de la Ley 1581 de 2012, no es necesario obtener la autorización previa del titular, no obstante, frente al cargo relacionado con el deber de informar la finalidad de la recolección de los datos, consideró la Dirección que la investigada era merecedora de una sanción.

Como es sabido, la Ley Estatutaria 1581 de 2012 ordena lo siguiente:

ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

(...)

b) **Principio de finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, **la cual debe ser informada al Titular**"

ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;

"ARTÍCULO 12. DEBER DE INFORMAR AL TITULAR. El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

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.

PARÁGRAFO. 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". (Énfasis añadido)

A su vez, el artículo 2.2.2.25.2.1 del Decreto Único Reglamentario 1074 de 2015, establece:

"Artículo 2.2.22.25.2.1. Recolección de los datos Personales. En desarrollo de los principios de finalidad y libertad, la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente. Salvo en los casos expresamente previstos en la Ley, no se podrán recolectar datos personales sin autorización del Titular.

A solicitud de la Superintendencia de Industria y Comercio, los Responsables deberán proveer 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.

No se podrán utilizar medios engañosos o fraudulentos para recolectar y realizar Tratamiento de datos personales". (destacamos)

En relación el principio de finalidad, la Corte Constitucional mediante sentencia C- 748 de 2011, manifestó:

"Principio de finalidad: En virtud de tal principio, el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley, la cual debe ser informada al titular.

La definición establecida por el legislador estatutario responde a uno de los criterios establecidos por la Corporación para el manejo de las bases de datos. Sin embargo, debe hacerse algunas precisiones.

Por una parte, los datos personales deben ser procesados con un propósito específico y explícito. En ese sentido, la finalidad **no sólo debe ser legítima** sino que la referida información se destinará a realizar los **fines exclusivos** para los cuales fue entregada por el titular. Por ello, se deberá informar al Titular del dato de manera clara, suficiente y previa acerca de la finalidad de la información suministrada y por tanto, no podrá recopilarse datos sin la clara especificación acerca de la finalidad de los mismos. Cualquier utilización diversa, **deberá ser autorizada en forma expresa por el Titular.**

Esta precisión es relevante en la medida que permite un control por parte del titular del dato, en tanto le es posible verificar si está siendo usado para la finalidad por él autorizada. Es una herramienta útil para evitar arbitrariedades en el manejo de la información por parte de quien trata el dato.

Así mismo, los datos personales deben ser procesados sólo en la forma que la persona afectada puede razonablemente prever. Si, con el tiempo, el uso de los datos personales cambia a formas que la persona razonablemente no espera, debe obtenerse el consentimiento previo del titular.

Por otro lado, de acuerdo la jurisprudencia constitucional y los estándares internacionales relacionados previamente, se observa que el principio de finalidad implica también: **(i) un ámbito temporal**, es decir que el período de conservación de los datos personales no exceda del necesario para alcanzar la necesidad con que se han registrado y **(ii) un ámbito material**, que exige que los datos recaudados sean los estrictamente necesarios para las finalidades perseguidas.

En razón de lo anterior, el literal b) debe ser entendido en dos aspectos.

Primero, bajo el principio de necesidad se entiende que los datos deberán ser conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos. Es decir, el periodo de conservación de los datos personales no debe exceder del necesario para alcanzar la necesidad con que se han registrado. (...)

Segundo, los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo de la base de datos. En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de datos personales al mínimo necesario. Es decir, los datos deberán ser: **(i) adecuados**, **(ii) pertinentes** y **(iii) acordes con las finalidades para las cuales fueron previstos**".

Conforme a lo anteriormente indicado, sólo podrá ser recolectada aquella información que sea **imprescindible** para cumplir con la **finalidad del tratamiento**, la cual deberá ser informada de manera clara y expresa al titular de la información, al momento en que es otorgada la autorización cuando sea necesaria. Si no lo es, en todo caso, se debe informar la finalidad específica del tratamiento.

La finalidad del tratamiento siempre se debe informar al titular del dato personal con independencia de si el tratamiento requiere o no de su autorización para que el mismo sea legítimo. En este sentido, el artículo 10 de la Ley Estatutaria 1581 de 2012 ordena que, "[q]uien acceda a los datos personales

sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley".

Así las cosas, **TUCONSULTA** estaba en la obligación de informar a los titulares la finalidad para la cual sus datos personales serían recolectados, independientemente que por efecto de la ley no sea obligatorio solicitar la autorización previa. Los titulares de la información tienen todo el derecho de conocer para qué serán tratados sus datos personales.

4. DE LAS ÓRDENES IMPARTIDAS EN LA RESOLUCIÓN No. 41383 DEL 2 DE JULIO DE 2021.

Con base en los hechos que dieron origen a la presente actuación administrativa y las pruebas **TUCONSULTA** recaudadas, la Dirección de Investigación de Protección de Datos Personales, consideró necesario impartir a las órdenes que se relacionan a continuación:

- La sociedad **TU CONSULTA COLOMBIA S.A.S.**, identificada con NIT 900.318.063-5, deberá retirar la selección por defecto en los diferentes checkbox habilitados en los formularios de inscripción que tiene dispuestos y que llegue a implementar en su página web, así como en los diferentes medios electrónicos que disponga para la recolección de datos, de acuerdo con lo dispuesto en la Ley 1581 de 2012 y el Decreto Único Reglamentario 1074 de 2015.
- La sociedad **TU CONSULTA COLOMBIA S.A.S.**, identificada con NIT 900.318.063-5, deberá en los formularios en los que pregunta ¿cuánto invierte en publicidad al año? Informar la Política de Tratamiento de Datos Personales y habilitar un mecanismo para que el Titular decida si acepta que su información se trate bajo lo dispuesto en ella.
- La sociedad **TU CONSULTA COLOMBIA S.A.S.**, identificada con NIT. 900.318.063-5, deberá implementar los mecanismos necesarios para garantizar que el Titular de la información consulte la Política de Protección de Datos Personales y sea informado de lo previsto en el artículo 12 de la Ley 1581 de 2012 cuando accede a los formularios de inscripción que tiene dispuestos y que llegue a implementar en su página web, así como en los diferentes medios electrónicos que disponga para la recolección de datos".

Respecto de las mismas, el **RECURRENTE** indicó lo siguiente:

Como se ha expresado a lo largo de las etapas procesales surtidas en el presente caso, tenemos implementado varios mecanismos para la recolección de los datos de nuestros visitantes y usuarios al sitio web de nuestra empresa y en la mayoría existía desde el momento en el que inicio esta investigación (Año 2017) los mecanismos de checkbox y elementos como el Recaptcha que permite garantizar que los mismos no sean diligenciados por robots u otros mecanismos similares.

La entidad en su afán de presentarnos como vulneradores de la norma, decide concentrarse en el único formulario (Que además solo funcionaba como trigger para el inicio frente a consultas) que no poseía el mecanismo de checkbox para la autorización. Esto lo advertimos a la entidad tanto en nuestros descargos como en el curso de la investigación, pero no fue tenido en cuenta. Si hoy se revisa el sitio web, todos los mecanismos señalados en la Resolución y que hoy son objeto de una orden administrativa por supuesto los tenemos implementados.

Si bien, la SIC insiste en que la autorización es el mecanismo fundamental para legitimar el tratamiento de los datos, no debe perderse de vista, que fenómenos como el comercio electrónico y la transformación digital han impuesto nuevas realidades para la captura de información sin que esta, per se, este precedida de un conocimiento siquiera del titular de los datos. Y a pesar que a ojos de la entidad esto suponga un reproche, es la forma, en que están configuradas tecnologías actuales. Así por ejemplo, la conexión a sitios web desde dispositivos, tienen como precedente, que se capturen datos y otros tipos de información como lugar de conexión, navegadores, fecha y hora por supuesto, de quien accede a un sitio web.

Sobre este punto en particular, resulta necesario traer a colación lo dispuesto en la Resolución No. 76538 del 27 de diciembre de 2019⁵, mediante la cual este Despacho se pronunció respecto del valor jurídico de las "políticas de privacidad" y del uso de medios electrónicos para obtener la autorización del titular del dato.

"Primero: El uso de mensajes de datos y de medios electrónicos es jurídicamente válido. Lo mismo sucede con la aceptación por conducta inequívoca-diferente al silencio- que permitan concluir de manera razonable que otorgó la autorización. La regulación también permite el uso de mecanismos "predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada".

Lo importante es que las tecnologías utilizadas, los procedimientos o mecanismos predeterminados se ajusten a las exigencias y los requerimientos probatorios de ley. Se reitera que es obligación de los Responsables del tratamiento utilizar tecnologías y procesos que permitan al Titular dar su consentimiento previo, expreso e informado, así como demostrar todo lo que exigen el ordenamiento jurídico.

⁵ Resolución mediante la cual se resolvió el recurso de apelación interpuesto dentro del radicado 16-409509.

Desde luego, el uso de tecnologías o procedimientos debe estar libre de cualquier medio engañoso o fraudulento para recolectar o Tratar datos personales, lo cual está proscrito por el artículo 4 del decreto 1377 de 2013 (Incorporado en el decreto 1074 de 2015).

Segundo: Usar la casilla "Checkbox" para aceptar "políticas de privacidad" no necesariamente significa que el Titular del dato autorizó el Tratamiento de su información. Esto se debe analizar en cada caso con miras a establecer, entre otras, lo siguiente:

- a) ¿El procedimiento utilizado permite comprobar la verdadera identidad de la persona que aceptó la política de privacidad? (Identidad plena del Titular del dato).
- b) ¿El consentimiento del Titular se obtuvo antes de la recolección y tratamiento de sus datos personales? (Consentimiento previo)
- c) ¿En el texto de la política de privacidad se informa todo lo que ordena el artículo 12 de la Ley 1581 de 2012? (Consentimiento informado)
- d) ¿El Responsable del Tratamiento conserva prueba del cumplimiento de lo previsto en el artículo 12 de la Ley 1581 de 2012 y está en capacidad de suministrar copia de la misma al Titular del dato?
- e) ¿Con el mecanismo o el procedimiento utilizado se puede establecer que el Titular del dato autorizó de manera expresa o mediante conductas inequívocas -diferentes al silencio-^{[19]6}
- f) ¿El Responsable del Tratamiento está en capacidad de suministrar plena prueba del consentimiento de cada Titular del dato?

Tercero: Aceptar "la política de privacidad" tampoco significa que la persona autorizó el tratamiento de su información.

La regulación colombiana no menciona expresamente el término "política de privacidad" sino que se refiere a los "avisos de privacidad" (AP) y a la "política de tratamiento de información" (PTI).

Nótese que el aviso de privacidad (en adelante AP) no es necesario aceptarlo ni tampoco usarlo. En efecto, según la regulación colombiana, éste sólo es necesario cuando "no sea posible poner a disposición del Titular las políticas de tratamiento de la información, los responsables deberán informar por medio de un aviso de privacidad al titular sobre la existencia de tales políticas y la forma de acceder a las mismas, de manera oportuna y en todo caso a más tardar al momento de la recolección de los datos personales"^{[20]7}

La función del aviso de privacidad^{[21]8} es la de dar a conocer a los Titulares la política de Tratamiento de información pero no la de reemplazar la obligación de obtener la autorización de la persona. Lo obligatorio es guardar copia del modelo de aviso de privacidad tal y como lo establece el artículo 16 del Decreto 1377 de 2013 (Incorporado en el Decreto 1074 de 2015):

"Deber de acreditar puesta a disposición del aviso de privacidad y las políticas de Tratamiento de la información. Los Responsables deberán 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. Para el almacenamiento del modelo, el Responsable podrá emplear medios informáticos, electrónicos o cualquier otra tecnología que garantice el cumplimiento de lo previsto en la Ley 527 de 1999".

La Política de Tratamiento de Información (en adelante PTI), por su parte, tampoco es necesario aceptarla. Lo que exige la regulación es que la misma sea "puestas en conocimiento de los titulares" tal y como lo ordena el artículo 13 del precitado decreto:

"Políticas de Tratamiento de la Información. Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.

Las políticas de Tratamiento de la información deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares. Dichas políticas deberán incluir, por lo menos, la siguiente información (...)^{[22]9}

⁶ [19] La figura de la conducta inequívoca fue incorporada en la regulación colombiana mediante el artículo 7 del decreto 1377 de 2013 en los siguientes términos: "Artículo 7°. Modo de obtener la autorización. Para efectos de dar cumplimiento a lo dispuesto en el artículo 9° de la Ley 1581 de 2012, los Responsables del Tratamiento de datos personales establecerán mecanismos para obtener la autorización de los titulares o de quien se encuentre legitimado de conformidad con lo establecido en el artículo 20 del presente decreto, que garanticen su consulta. Estos mecanismos podrán ser predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste (i) por escrito, (ii) de forma oral o (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca". (Destacamos)

⁷ [20] Cfr. Artículo 14 Del Decreto 1377 de 2013 (Incorporado en el artículo 2.2.25.3.3 Decreto 1074 de 2015)-

⁸ [21] Según el artículo 15 del Decreto 1377 de 2013 (Incorporado en el artículo 2.2.25.3.4. Decreto 1074 de 2015) "El aviso de privacidad, como mínimo, deberá contener la siguiente información:

1. Nombre o razón social y datos de contacto del responsable del tratamiento.
2. El tratamiento al cual serán sometidos los datos y la finalidad del mismo.
3. Los derechos que le asisten al titular.

4. Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información y los cambios sustanciales que se produzcan en ella o en el Aviso de Privacidad correspondiente. En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de Información.

No obstante lo anterior, cuando se recolecten datos personales sensibles, el aviso de privacidad deberá señalar expresamente el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos.

En todo caso, la divulgación de Aviso de Privacidad no eximirá al Responsable de la obligación de dar a conocer a lo titulares la política de tratamiento de la información, de conformidad con lo establecido en este decreto"

⁹ [22] Según el artículo 12 del Decreto 1377 de 2013 (incorporado en el artículo 2.2.25.3.1 Decreto 1074 de 2015), la Política de Tratamiento de información debe contener, como mínimo, lo siguiente:

- "1. Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.

2. Tratamiento al cual serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.

Aceptar la PTI no implica que el Titular del dato esté autorizando el Tratamiento de su información.

En suma, aceptar el AP o PTI no es imperativo ni releva per se, al Responsable de obtener la autorización previa, expresa e informada del Titular. Basta recordar las siguientes normas que ponen de presente la necesidad de contar el consentimiento de la persona cuya información era objeto de tratamiento:

- "El Tratamiento sólo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento" ^[23]¹⁰
- "(...) en el Tratamiento se requiere la autorización previa e informada del titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior" ^[24]¹¹
- "Los Responsables deberán conservar prueba de la autorización otorgada por los Titulares de datos personales para el Tratamiento de los mismos" ^[25]¹²
- Es derecho del cliente o de cualquier personal (Titular del Dato): "Solicitar prueba de la autorización otorgada al Responsable del Tratamiento" ^[26]¹³

Conforme a lo anterior, los Responsables del tratamiento están habilitados para construir a través de herramientas tecnológicas, espacios en los que los titulares de información puedan de una manera clara, transparente y expedita autorizar el tratamiento de sus datos personales, conforme a las normas de protección de datos.

No obstante, y de acuerdo con el Acta de Análisis de Expedientes relacionada en el oficio No. 17-154376-34 del 12 de agosto de 2020, al abrir cada uno de los enlaces enviados por parte de **TUCONSULTA** cuando da respuesta a las pruebas decretadas en la Resolución No. 9541 del 3 de marzo de 2020, los formularios reportados contienen un mecanismo de aceptación de políticas de privacidad y de tratamiento de datos personales consistente en un **Checkbox, el cual se encuentra activado por defecto**. En este orden de ideas, dentro de los mecanismos tecnológicos implementados por parte de **TUCONSULTA**, da por sentado que con el conocimiento de las "políticas de privacidad" o "la política de tratamiento de datos personales" e inclusive con el "Aviso de Privacidad", se subsana el derecho que tiene el titular de autorizar de manera previa el tratamiento de sus datos.

Aunque es válido la utilización de los Checkbox para el tratamiento de los datos personales, el Responsable del Tratamiento debe dar la oportunidad al titular de conocer las finalidades del tratamiento de su información, para que así pueda autorizar de manera previa su tratamiento. Y, desde luego, debe permitir que sea la persona quien decida libremente si autoriza o no la recolección y uso de su información.

Así las cosas, este Despacho modificará la orden impartida por parte de la Dirección de Investigación de Protección de Datos Personales, para que **TUCONSULTA** realice las modificaciones técnicas necesarias para que el Checkbox que se encuentra habilitado en cada uno de los formularios que fueron allegados a la presente actuación administrativa se ajusten a los principios y deberes establecidos en la Ley 1581 de 2012, informando al titular la finalidad por la cual su información está siendo recolectada, para que pueda autorizar su tratamiento de manera previa.

5. POTESTAD SANCIONADORA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Según la Corte Constitucional, "es innegable que a través del derecho administrativo sancionador se pretende garantizar la preservación y restauración del ordenamiento jurídico, mediante la imposición de una sanción que no sólo repruebe sino que también prevenga la realización de todas aquellas conductas contrarias al mismo. Se trata, en esencia, de un poder de sanción ejercido por las autoridades administrativas que opera ante el incumplimiento de los distintos mandatos que las normas jurídicas imponen a los administrados y aún a las mismas autoridades públicas"¹⁴.

3. Derecho que le asisten como Titular.

4. Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.

5. Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información revocar la autorización.

6. Fecha de entrada en vigencia de la política de tratamiento de la información y periodo de vigencia de la base de datos (...)"

¹⁰ [23] Cfr. Literal c) del artículo 4 de la Ley 1581 de 2012.

¹¹ [24] Cfr. Artículo 9 de la Ley 1581 de 2012.

¹² [25] Cfr. Artículo 8 del Decreto 1377 de 2013 (Incorporado en el artículo 2.2.2.25.2.6 Decreto 1074 de 2015)

¹³ [26] Cfr. Literal b) del artículo 8 de la Ley 1581 de 2012

¹⁴ Cfr. Corte Constitucional, sentencia C-818 del 9 de agosto de 2005. MP. Dr. Rodrigo Escobar Gil. En:

<https://www.corteconstitucional.gov.co/relatoria/2005/C-818-05.htm>

Frente al procedimiento para imponer las sanciones, el artículo 22 de la Ley 1581 de 2012 señala que, *"La Superintendencia de Industria y Comercio, una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento, adoptará las medidas o impondrá las sanciones correspondientes (...)"*.

El artículo 23¹⁵, por su parte, establece las sanciones que podrá imponer esta entidad a los Responsables y Encargados del Tratamiento de Datos.

Respecto de la "Potestad sancionatoria", la Corte Constitucional ha señalado:

"El poder sancionador estatal ha sido definido como "un instrumento de autoprotección, en cuanto contribuye a preservar el orden jurídico institucional mediante la asignación de competencias a la administración que la habilitan para imponer a sus propios funcionarios y a los particulares el acatamiento, inclusive por medio punitivos, de una disciplina cuya observancia contribuye a la realización de sus cometidos.

Esa potestad es una manifestación del jus punendi, razón por la que está sometida a los siguientes principios: (i) el principio de legalidad, que se traduce en la existencia de una ley que la regule; es decir, que corresponde sólo al legislador ordinario o extraordinario su definición. (ii) El principio de tipicidad que, si bien no es igual de riguroso al penal, sí obliga al legislador a hacer una descripción de la conducta o del comportamiento que da lugar a la aplicación de la sanción y a determinar expresamente la sanción. (iii) El debido proceso que exige entre otros, la definición de un procedimiento, así sea sumario, que garantice el debido proceso y, en especial, el derecho de defensa, lo que incluye la designación expresa de la autoridad competente para imponer la sanción. (iv) El principio de proporcionalidad que se traduce en que la sanción debe ser proporcional a la falta o infracción administrativa que se busca sancionar. (v) La independencia de la sanción penal; esto significa que la sanción se puede imponer independientemente de si el hecho que da lugar a ella también puede constituir infracción al régimen penal."¹⁶

En el mismo sentido, y en relación con los principios¹⁷ señalados, dicha corporación por medio de la Sentencia C-948 de 2002 manifestó:

"En la doctrina^[36]¹⁸ se postula, así mismo, sin discusión que la administración o las autoridades titulares de funciones administrativas lo sean de potestad sancionadora y que ésta en cuanto manifestación del ius puniendi del Estado está sometida a claros principios generalmente aceptados, y en la mayoría de los casos proclamados de manera explícita en los textos constitucionales. Así, a los principios de configuración del sistema sancionador como los de legalidad (toda sanción debe tener fundamento en la ley), tipicidad (exigencia de descripción específica y precisa por la norma creadora de las infracciones y de las sanciones, de las conductas que pueden ser sancionadas y del contenido material de las sanciones que puede imponerse por la comisión de cada conducta, así como la correlación entre unas y otras) y de prescripción (los particulares no pueden quedar sujetos de manera indefinida a la puesta en marcha de los instrumentos sancionatorios), se suman los propios de aplicación del sistema sancionador, como los de culpabilidad o responsabilidad según el caso – régimen disciplinario o régimen de sanciones administrativas no disciplinarias- (juicio personal de reprochabilidad dirigido al autor de un delito o falta^[37] ¹⁹), de proporcionalidad o el denominado non bis in ídem".

Ahora, al hacer referencia al principio de legalidad en materia de protección del derecho de habeas data, la Corte Constitucional mediante Sentencia C-1011 de 2008, manifestó:

"Para la Corte, en consecuencia, la flexibilidad que puede establecer el legislador en materia de derecho administrativo sancionador es compatible con la Constitución, siempre que esta característica no sea tan amplia que permita la arbitrariedad de la administración. Un cierto grado de movilidad a la administración para aplicar las hipótesis fácticas establecidas en la ley guarda coherencia con los fines constitucionales de esta actividad sancionatoria administrativa, en la medida que le permite cumplir eficaz y eficientemente con las obligaciones impuestas por la Carta. Sin embargo, ha advertido que la flexibilidad del principio de

¹⁵ **ARTÍCULO 23. SANCIONES.** La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

- 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;
- 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;
- 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;
- Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

¹⁶ Corte Constitucional. Sentencia C-748 de 2011

¹⁷ "Los principios señalados en el CPACA tienen un carácter normativo y vinculante, a diferencia de la naturaleza orientadora que se predicaba en el CCA. La aplicabilidad general de los principios previstos en el artículo 3° del CPACA, como desarrollo directo de la Constitución Política, conlleva a que dichos principios deban observarse para cualquier actuación administrativa, incluidas las reguladas en leyes especiales. Así las cosas, el intérprete deberá utilizarlos directamente o hacer un ejercicio de integración normativa, entre los principios de la actuación administrativa previstos en la ley especial y los señalados en el CPACA". Laverde A. JUAN MANUEL. Manual de Procedimiento Administrativo Sancionatorio. Ed. Legis S.A. Bogotá Colombia Segunda Edición 2018.p. 51

¹⁸ [36] Juan Alfonso Santamaría Pastor. Principios de Derecho Administrativo. Volumen II. Ed. Centro de Estudios Ramón Areces. Madrid. Tomo II. Segunda Edición. 2000.

¹⁹ [37] Ver Ramón Parada Vásquez. Derecho Administrativo. Tomo I Marcial Pons. Madrid 1996. Luis Morell Ocaña. Curso de Derecho Administrativo. Tomo II "La actividad de las administraciones públicas. Su control administrativo y jurisdiccional". Arandazi. Madrid. 1996.

legalidad no puede tener un carácter extremo, al punto que se permita la arbitrariedad de la administración en la imposición de las sanciones o las penas^[203]²⁰.

Por lo tanto, no puede la administración sobrepasar los límites que le impone el legislador al momento de aplicar una sanción, es decir, que la conducta que está siendo investigada debe tener una connotación sancionable por mandato legal. En este punto es relevante el **principio de tipicidad**, el cual no es otra cosa que *“la exigencia de una descripción específica y precisa por la norma creadora de las infracciones y de las sanciones, de las conductas que pueden ser sancionadas y del contenido material de las sanciones que puede imponerse por la comisión de cada conducta, así como la correlación entre unas y otras”²¹.*

Sobre el citado principio de tipicidad, la Corte Constitucional mediante Sentencia C - 748 de 2011 sostuvo:

*“En relación con el principio de tipicidad, encuentra la Sala que pese a la generalidad de la ley, es determinable la infracción administrativa en la medida en que se señala que la constituye el **incumplimiento de las disposiciones de la ley**, esto es, en términos específicos, la regulación que hacen los artículos 17 y 18 del proyecto de ley, en los que se señalan los deberes de los responsables y encargados del tratamiento del dato”.*

Se concluye entonces que es suficiente desconocer cualquiera de las disposiciones contempladas en la Ley 1581 de 2012, para que la administración pueda ejercer su potestad sancionatoria, eso sí, en los casos en los que así lo determine la actuación administrativa correspondiente, como consecuencia directa de la trasgresión de las normas que amparan el derecho fundamental de *habeas data*. Principalmente, cuando se trata de las disposiciones que se refieren a los deberes a los que están sujetos los Responsables o Encargados del Tratamiento de la información.

Así las cosas, en el caso bajo estudio, se dan los presupuestos requeridos para determinar que **TUCONSULTA**, en calidad de Responsable del Tratamiento, vulneró las normas de protección del derecho de *habeas data* relacionadas con el principio de libertad, al no informar la finalidad por la cual la información sería recolectada en los diferentes formularios que se encuentran en su página web.

Por su parte, el artículo 24, ordena que *“las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:*

- a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;*
- b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;*
- c) La reincidencia en la comisión de la infracción;*
- d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;*
- e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio;*
- f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.*

Como se observa, este último establece los factores o elementos de juicio pertinentes que, según las particularidades de cada caso, se deben aplicar para imponer una sanción, respetando las garantías del artículo 29 constitucional²². Esos criterios, según la Sentencia C-748 de 2011, hacen referencia a cinco circunstancias de agravación, entre los literales a) y e), **y a una de atenuación o disminución de la sanción, correspondiente al literal f).**

Conforme a lo anterior, y en la medida que **TUCONSULTA** a lo largo de la presente actuación administrativa, no aceptó de manera expresa la comisión de la falta que se le imputa, razón por la cual no es procedente acceder a la solicitud de disminuir la sanción impuesta.

Es necesario precisar que las sanciones que se imponen dentro de procesos administrativos sancionatorios no constituyen ninguna cuantificación de perjuicios materiales o morales, es decir no se trata de la estimación de un daño subjetivo, como sucede en el régimen civil de responsabilidad.

²⁰ [203] Sentencia C-406 de 2004.

²¹ Sentencias C-827 de 2001 y C-343 de 2006.

²² Artículo 29. El debido proceso se aplicará a toda clase de actuaciones judiciales y **administrativas**. (...) (negrita añadida)

Por el contrario, las sanciones que impone esta superintendencia, en virtud del artículo 22 de la Ley 1581 de 2012, son una consecuencia contra la persona natural o jurídica que viole las disposiciones de la citada ley²³. Ese efecto negativo tiene como finalidad no solo sancionar por violar las leyes sino promover y garantizar el cumplimiento del Régimen General de Protección de Datos Personales y, de esa forma, proteger el Derecho Fundamental a la Protección de Datos Personales, entre otros²⁴.

La imposición de sanciones por violación de la Ley 1581 de 2012 tiene como fin central proteger y promover el respeto del derecho fundamental a la protección de Datos personales, derecho humano (universal, inalienable, indivisible, irrenunciable e imprescriptible) que fue positivizado en el artículo 15 de la Constitución Política Nacional, y que, en muchas ocasiones es conexo a otros derechos fundamentales de gran relevancia constitucional como la dignidad humana; el buen nombre; la intimidad; etc.

Del mismo modo, la vulneración del Derecho Fundamental a la Protección de Datos Personales no solo afecta los derechos de una persona en particular, sino que, pone en riesgo los derechos fundamentales de toda la sociedad. Por eso, las sanciones de dichas conductas no pueden, ni deben tratarse, como una cuestión insignificante o de poca monta. La transgresión flagrante a los derechos humanos de un ciudadano es, por sí solo, un hecho muy grave que no necesita de forzosos razonamientos para comprender su notoria importancia en la sociedad.

De conformidad con lo indicado, la sanción impuesta es proporcional si se tiene en cuenta que el monto límite de las sanciones establecido en el artículo 23 de la Ley 1581 de 2012 es de dos mil (2000) salarios mínimos legales mensuales vigentes, por lo que, la multa impuesta a **TUCONSULTA** corresponde al 0.17% del límite dispuesto en la ley.

Finalmente, resulta pertinente resaltar lo siguiente:

- a) La multa impuesta a **TUCONSULTA** corresponde al 0.17% del máximo legal permitido (2000 salarios mínimos legales mensuales vigentes establecido en el artículo 23 de la Ley 1581 de 2012).
- b) El monto de dicha sanción es el resultado del análisis del daño y/o puesta en peligro de los intereses jurídicos tutelados en el trámite de la primera instancia de esta actuación administrativa. Así como del incumplimiento de los deberes impuestos por la Ley 1581 de 2012 a los Responsables y Encargados del Tratamiento de los Datos personales.
- c) La Resolución recurrida fue proferida con la debida observancia de los principios que rigen las actuaciones administrativas. Asimismo, fue el resultado de la valoración fáctica y probatoria de la primera instancia que llevó a concluir y comprobar la vulneración al derecho de *habeas data* del Titular y en particular de los mandatos legales señalados.
- d) Las sanciones que se imponen dentro de esta clase de procesos, no derivan de los daños o perjuicios causados a los Titulares por incumplir la regulación sobre Tratamiento de Datos personales. Es decir, las normas que protegen el derecho de *habeas data* o protección de Datos personales no se refieren a la responsabilidad civil de los Responsables y Encargados del Tratamiento de Datos.
- e) La vulneración del derecho de *habeas data* o la protección de datos personales no solo afecta al Titular, también pone en riesgo los derechos de toda la sociedad. Por esto, las sanciones no pueden ni deben tratarse como una cuestión insignificante o de poca cuantía, ni mucho menos como si las incidencias del proceso lo convirtieran en uno de indemnización de daños y perjuicios. Esto, en razón a que existe de por medio una trasgresión flagrante a los derechos humanos de un ciudadano, lo cual es suficiente para entender la gravedad de la conducta, sin

²³ El artículo 22 de la Ley 1581 de 2012 define que la Superintendencia de Industria y Comercio, **una vez establecido el incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento**, adoptará las medidas o impondrá las sanciones correspondientes. (negrita añadida). Al respecto dijo la Corte Constitucional en la Sentencia C-748 de 2011: "*Esta norma [el artículo 23] cumple con el principio de tipicidad, para lo cual debe interpretarse conjuntamente con el artículo 22 de la futura ley estatutaria, que establece la posibilidad de imponer sanciones cuando se hayan incumplido las disposiciones de esta ley. En este sentido, el supuesto de hecho que completa la norma jurídica sancionatoria está constituido por la infracción de las disposiciones de la futura ley estatutaria por la cual se dictan disposiciones generales para la protección de datos personales.*" (negrita añadida)

²⁴ Las sanciones impuestas en función del derecho administrativo sancionatorio pretenden asegurar el orden público y el correcto funcionamiento de la administración. Al respecto ver: Corte Constitucional, Sala Plena, C-703 de 2010, Magistrado Ponente Gabriel Eduardo Mendoza, Considerando 5; Corte Constitucional, Sala Plena, C-010-03, Magistrada Ponente Clara Inés Vargas.

necesidad de acudir a forzosos razonamientos o teorías complicadas, a fin de desentender o negar una verdad inconcusa, cual es la del quebrantamiento de derechos constitucionales.

Recuérdese que, según la Declaración Universal de los Derechos Humanos, *“el desconocimiento y el menosprecio de los derechos humanos han originado actos de barbarie ultrajantes para la conciencia de la humanidad”*²⁵. Por eso, según dicho documento, se considera *“esencial que los derechos humanos sean protegidos por un régimen de Derecho”*. No debe olvidarse que el respeto de los Derechos Humanos es un elemento esencial de la democracia²⁶. Así las cosas, recalcamos, la violación de Derechos Humanos es una conducta gravísima que no solo atenta contra los intereses de un individuo en particular sino de la sociedad en general.

Con apoyo en estos argumentos, no se acogerán las consideraciones de la recurrente en la medida en que la sanción impuesta se ajusta a derecho y obedece a las particularidades propias de esta actuación administrativa.

6. RESPONSABILIDAD DEMOSTRADA (ACCOUNTABILITY) Y “COMPLIANCE” EN EL TRATAMIENTO DE DATOS PERSONALES

La regulación colombiana le impone al Responsable del Tratamiento la responsabilidad de garantizar la eficacia de los derechos del Titular del Dato, la cual no puede ser simbólica ni formal, sino real y demostrable. Téngase presente que según nuestra jurisprudencia *“existe un deber constitucional de administrar correctamente y de proteger los archivos y bases de datos que contengan información personal o socialmente relevante”*²⁷.

Adicionalmente, los Responsables o Encargados del Tratamiento no son dueños de los Datos personales que reposan en sus Bases de Datos o archivos. En efecto, ellos son meros tenedores que están en el deber de administrar de manera correcta, apropiada y acertada la información de las personas porque su negligencia o dolo en esta materia afecta los derechos humanos de los Titulares de los Datos.

En virtud de lo anterior, el capítulo III del Decreto 1377 del 27 de junio de 2013 -incorporado en el Decreto 1074 de 2015- reglamenta algunos aspectos relacionados con el principio de responsabilidad demostrada.

El artículo 26²⁸ -titulado DEMOSTRACIÓN- establece que *“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”*. Así resulta imposible ignorar la forma en que el Responsable o Encargado del Tratamiento debe probar poner en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación. Es decir, se reivindica que un administrador no puede utilizar cualquier tipo de políticas o herramientas para dicho efecto, sino solo aquellas que tengan como propósito lograr que los postulados legales sean realidades verificables, y no solo se limiten a creaciones teóricas e intelectuales.

Con el propósito de dar orientaciones sobre la materia, la Superintendencia de Industria y Comercio expidió el 28 de mayo de 2015 la *“Guía para implementación del principio de responsabilidad demostrada (accountability)”*²⁹.

²⁵ Organización de las Naciones Unidas (1948). Declaración Universal de los Derechos Humanos.

²⁶ Artículo 3 de la Carta Democrática Interamericana la cual se puede consultar en: http://www.oas.org/OASpage/esp/Documentos/Carta_Democratica.htm

²⁷ Cfr. Corte Constitucional, sentencia T-227 de 2003

²⁸ El texto completo del artículo 26 del decreto 1377 de 2013 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, en una manera que sea proporcional a lo siguiente:

1. La naturaleza jurídica del responsable 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 personales objeto del tratamiento.
3. El tipo de Tratamiento.
4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.

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 personales, como también la descripción de las finalidades para las cuales esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso. En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas”

²⁹ El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

El término “*accountability*” a pesar de los diferentes significados ha sido entendido en el campo de la protección de Datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, y la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente.

Conforme con ese análisis, las recomendaciones que trae la guía a los obligados a cumplir la ley 1581 de 2012:

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

El principio de responsabilidad demostrada –*accountability*– demanda implementar acciones de diversa naturaleza³⁰ 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 implementen medidas apropiadas, efectivas y verificables que le permitan evidenciar la observancia de las normas sobre la materia.

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

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

En este sentido, desde el año 2006 la Red Iberoamericana de Protección de Datos (RIPD) ha puesto de presente que *“la autorregulación sólo redundará en beneficio real de las personas en la medida que sea bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que **no se constituyan en meras declaraciones simbólicas de buenas intenciones sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales**”*³¹. (Destacamos).

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 capaces de garantizar los derechos de los Titulares de los Datos personales y su gestión siempre sea respetuosa de los derechos humanos.

Aunque no es espacio para explicar cada uno de los anteriores aspectos mencionados en la guía³², ponemos de presente que el principio de responsabilidad demostrada se articula con el concepto de “*compliance*” en la medida que este hace referencia al “*conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y*

³⁰ Estas medidas pueden ser de naturaleza administrativa, organizacional, estratégica, tecnológica, humanas y de gestión que involucran procesos y procedimientos.

³¹ 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.

³² El texto de la guía puede consultarse en: <http://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf>

legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos"³³.

También se ha afirmado que "compliance es un término que hace referencia a la gestión de las organizaciones conforme a las obligaciones que le vienen impuestas (requisitos regulatorios) o que se ha autoimpuesto (éticas)"³⁴. Adicionalmente, se precisa que ya no vale solo intentar cumplir la ley sino que las organizaciones deben asegurarse que se cumple y deben generar evidencias de sus esfuerzos por cumplir y hacer cumplir a sus miembros, bajo la amenaza de sanciones si no son capaces de ello. Esta exigencia de sistemas más eficaces impone la creación de funciones específicas y metodologías de compliance³⁵.

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

La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales del *compliance* y buena parte de lo que implica el principio de responsabilidad demostrada (*accountability*). En la mencionada guía se considera fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un "sistema de administración de riesgos asociados al tratamiento de datos personales"³⁶ que les permita "identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales"³⁷.

Finalmente, 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."³⁸
(Destacamos)

Conforme a lo anterior los Responsables del tratamiento de datos personales deben estar en la capacidad de demostrar que cumplen con los procedimientos necesarios para garantizar el ejercicio del derecho de habeas data, en el presente caso, en lo que tiene que ver con el principio de libertad.

7. RESPONSABILIDAD DE LOS ADMINISTRADORES EN MATERIA DE TRATAMIENTO DE DATOS PERSONALES

El 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, entre otros, la protección de los derechos humanos porque son imprescindibles para que cualquier ser humano sea tratado como una "persona" y no como un objeto o cosa.

³³ Cfr. World Compliance Association (WCA). <http://www.worldcomplianceassociation.com/> (última consulta: 6 de noviembre de 2018)

³⁴ Cfr. Bonatti, Francisco. Va siendo hora que se hable correctamente de compliance (III). Entrevista del 5 de noviembre de 2018 publicada en Canal Compliance: <http://www.canal-compliance.com/2018/11/05/va-siendo-hora-que-se-hable-correctamente-de-compliance-iii/>

³⁵ Idem

³⁶ Cfr. Superintendencia de Industria y Comercio (2015) "Guía para implementación del principio de responsabilidad demostrada (*accountability*)". Págs 16-18

³⁷ Ibid. P 16

³⁸ 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>

En línea con lo anterior, nuestra Constitución Política Nacional recalca 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 *“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 precitado 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 Política pone de presente que la participación en el mercado supone responsabilidades y que efectuar actividades empresariales implica cumplir con las obligaciones previstas en la ley.

Según el artículo 22 de la ley 222 de 1995³⁹ 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”*. (Destacamos)

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 cumplimiento en todas las actividades que realiza su empresa u organización.

El artículo 24⁴⁰ de la Ley 222 de 1995, presume la culpa del administrador *“en los casos de incumplimiento o exlimitación de sus funciones, violación de la ley o de los estatutos”*. Dicha 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.

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 El texto completo del artículo 24 de la ley 222 de 1995 dice lo siguiente: *“Artículo 24. 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 exlimitación 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

Sin perjuicio de lo establecido, no se accederá a las pretensiones del **RECURRENTE**, por, entre otras, las siguientes razones:

1. La finalidad de tratamiento siempre se debe informar al titular del dato personal con independencia de si se requiere o no de autorización para que el mismo sea legítimo. En este sentido, el artículo 10 de la Ley Estatutaria 1581 de 2012 ordena que, "[q]uien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley".
2. **TUCONSULTA** incumplió con el deber establecido en el literal c) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal b) del artículo 4 y el artículo 12 de la misma norma, pues no informa a los titulares las finalidades por las cuales se está recolectando los datos personales.
3. La multa impuesta a TUCONSULTA corresponde al 0.17% del máximo legal permitido (2000 salarios mínimos legales mensuales vigentes establecido en el artículo 23 de la Ley 1581 de 2012).
4. Las casillas "pre marcadas" por defecto, no constituye consentimiento bajo la Ley 1581 de 2012, En esas situaciones, no es posible determinar de manera objetiva si el titular ha dado o no su consentimiento sobre la base de una decisión libre e informada.
5. El uso de mensajes de datos y de medios electrónicos es jurídicamente válido. Lo mismo sucede con la aceptación por conducta inequívocas -*diferentes al silencio*- que permitan concluir de forma razonable que otorgó la autorización. La regulación también permite el uso de mecanismos "*predeterminados a través de medios técnicos que faciliten al Titular su manifestación automatizada*".

Lo importante es que las tecnologías utilizadas, los procedimientos o mecanismos predeterminados se ajusten a las exigencias legales y los requerimientos probatorios de ley. Se reitera que es obligación de los Responsables del tratamiento utilizar tecnologías y procesos que permitan al Titular dar su consentimiento previo, expreso e informado, así como demostrar todo lo que exige el ordenamiento jurídico⁴².

6. Usar una casilla "Checkbox" para aceptar "políticas de privacidad" no necesariamente significa que el titular del dato autorizó el Tratamiento de su información. Esto debe analizar en cada caso con miras a establecer, entre otras, lo siguiente:
 - a) ¿El procedimiento utilizado permite comprobar la verdadera identidad de la persona que aceptó la política de privacidad? (Identidad plena del Titular del dato).
 - b) ¿El consentimiento del Titular se obtuvo antes de la recolección y tratamiento de sus datos personales? (Consentimiento previo)
 - c) ¿En el texto de la política de privacidad se informa todo lo que ordena el artículo 12 de la Ley 1581 de 2012? (Consentimiento informado)
 - d) ¿El Responsable del Tratamiento conserva prueba del cumplimiento de lo previsto en el artículo 12 de la Ley 1581 de 2012 y está en capacidad de suministrar copia de la misma al Titular del dato?
 - e) ¿Con el mecanismo o el procedimiento utilizado se puede establecer que el Titular del dato autorizó de manera expresa o mediante conductas inequívocas -*diferentes al silencio*-
 - f) ¿El Responsable del Tratamiento está en capacidad de suministrar plena prueba del consentimiento de cada Titular del dato?⁴³
7. Aceptar "la política de privacidad" tampoco significa que la persona autorizó el tratamiento de su información. La regulación colombiana no menciona expresamente el término "política de privacidad" sino que se refiere a los avisos de privacidad y a la política de tratamiento de información.⁴⁴
8. **TUCONSULTA** deberá ajustar los mecanismos predeterminados en los formularios que tenga dispuestos en su página web, de conformidad con la Ley 1581 de 2012, para que el titular de la

⁴² Resolución No. 76538 del 27 de diciembre de 2019.

⁴³ Ibidem

⁴⁴ Ibidem

información se informe y pueda autorizar el tratamiento de sus datos personales de manera previa.

De conformidad con lo anterior y una vez analizadas las pruebas y documentos allegados a la presente actuación administrativa, encuentra este Despacho que el acto administrativo objeto de impugnación fue expedido observando la Ley. De esta forma y de acuerdo con el artículo 80 del Código de Procedimiento Administrativo y lo Contencioso Administrativo y las consideraciones del Despacho, se confirmará la Resolución No. 75827 de 26 de noviembre de 2020.

En mérito de lo expuesto, este Despacho,

RESUELVE

PRIMERO: CONFIRMAR el **ARTÍCULO PRIMERO** de la Resolución No. 41383 del 2 de julio de 2021 de conformidad con lo expuesto en la parte motiva del presente acto administrativo.

SEGUNDO: MODIFICAR el **ARTÍCULO SEGUNDO** de la Resolución No. 41383 del 2 de julio de 2021, el cual quedará así:

ARTÍCULO SEGUNDO: ORDENAR a la sociedad **TU CONSULTA COLOMBIA S.A.S.**, identificada con NIT. 900.318.063-5, que dentro del término de **DOS (2) MESES** siguientes a la ejecutoria de la presente decisión, ajuste los mecanismos que tenga predeterminados en los diferentes formularios dispuestos en su página web, para garantizar que el titular conozca y se informe respecto las finalidades específicas del tratamiento que se le dará a sus datos personales.

SEGUNDO: Notificar personalmente en contenido de la presente decisión a la sociedad **TU CONSULTA COLOMBIA S.A.S.**, identificada con el Nit. 900.318.063-5, a través de su Representante Legal o su apoderado, entregándole copia de la misma e informándole que contra el presente acto administrativo no procede recurso alguno.

TERCERO: Comunicar la presente decisión al señor [REDACTED], identificado con la cédula de ciudadanía No. [REDACTED].

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

NOTIFÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., noviembre 19 de 2021

El Superintendente Delegado para la Protección de Datos Personales,

**NELSON
REMOLINA
ANGARITA**

Firmado
digitalmente por
NELSON
REMOLINA
ANGARITA
Fecha: 2021.11.19
15:03:14 -05'00'

NELSON REMOLINA ANGARITA

NOTIFICACIÓN

Entidad: TUCONSULTA COLOMBIA S.A.S.
Identificación: Nit. No. 900.318.063-5
Representante Legal: Jorge Fernando Concha Jaramillo
Identificación: C.C. 79.460.644
Dirección: Calle 116 A No. 70D – 14 Piso 1
Ciudad: Bogotá D.C.
Correo Electrónico: contabilidad@novoclick.net

COMUNICACIÓN**Titular de la información:**

Nombre: [REDACTED]
Identificación: C.C. No. [REDACTED]
Correo electrónico: [REDACTED]