LA PROTECCIÓN DE DATOS EN COLOMBIA DURANTE LA DECLARATORIA DE LA EMERGENCIA SANITARIA A CAUSA DEL CORONAVIRUS COVID – 19

ANDRÉS FELIPE PIANDA AGREDA

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE DERECHO

DEPARTAMENTO DE CIENCIAS JURÍDICAS

SANTIAGO DE CALI, 15 DE MAYO DE 2023

LA PROTECCIÓN DE DATOS EN COLOMBIA DURANTE LA DECLARATORIA DE LA EMERGENCIA SANITARIA A CAUSA DEL CORONAVIRUS COVID – 19

Andrés Felipe Pianda Agreda

Trabajo de grado dirigido por:

Dr. Luis Félix Barriga Palomino

PONTIFICIA UNIVERSIDAD JAVERIANA

FACULTAD DE CIENCIAS JURÍDICAS

MAESTRÍA EN DERECHO EMPRESARIAL

SANTIAGO DE CALI, MAYO DE 2023

DEDICATORIA

A mi extensa familia biológica, especialmente a mis padres que me inspiraron para tomar este camino y a mis abuelos que me guían desde las alturas.

A mi familia elegida, la escogida, la que me regaló la vida.

AGRADECIMIENTOS

Agradezco al Dr. Luis Félix Barriga Palomino; Docente de la facultad de Ciencia Jurídica y Política de la Pontificia Universidad Javeriana Cali, por las horas dedicadas a la dirección del presente trabajo, por sus aportes invaluables y su visión sobre la problemática planteada.

Finalmente agradezco a los distintos profesionales, colegas y amigos por sus distintas contribuciones y aportes para la construcción del presente escrito.

Tabla de Contenido

Resumen

El presente trabajo de investigación realiza un análisis dogmático de como se desarrollaron las facultades de inspección, vigilancia y control para garantizar el tratamiento de datos personales por parte de la Superintendencia de Industria y Comercio en el tiempo que transcurrió la emergencia sanitaria a causa del Coronavirus Covid – 19. Para ello, se analizó 150 Resoluciones que se emitieron desde la Resolución 385 del 12 de marzo del año 2020 hasta el 31 de diciembre del año 2021. En este contexto se observaron el estado del trámite, los fundamentos normativos como la Ley 1581 de 2012, los principales criterios jurídicos que determinan la decisión final y estas. En ello, se encuentra que la SIC tuvo un papel activo y garante en la protección del derecho fundamental del Habas Data; tomó medidas preventivas cuando este se encontraba en riesgo y no se había probado una vulneración; evidenciando que en la mayoría de las resoluciones había peligro para los intereses jurídicos tutelados por la ley de Protección de Datos Personales.

Palabras Claves: Habeas Data, Protección de Datos Personales, Apps, Ley 1581 de 2012, Coronavirus Covid – 19, Superintendencia de Industria y Comercio.

Abstract

This research work carries out a dogmatic analysis of how the inspection, surveillance and control powers were developed to guarantee the processing of personal data by the Superintendency of Industry and Commerce during the time that the health emergency elapsed due to the Coronavirus Covid – 19. For this, 150 Resolutions that were issued from Resolution 385 of March 12, 2020 to December 31, 2021 were analyzed. In this context, the status of the process, the regulatory foundations such as Law 1581 were observed. of 2012, the main legal criteria that determine the final decision and these. In this, it is found that the SIC had an active and guarantor role in the protection of the fundamental right of Habas Data; took preventative measures when it was at risk and a breach had not been proven; evidencing that in most of the resolutions there was danger to the legal interests protected by the Personal Data Protection law.

Keywords: Habeas Data, Protection of Personal Data, Apps, Law 1581 of 2012, Coronavirus COVID-19, Superintendence of Industry and Commerce

Introducción

En este contexto se plantea la siguiente pregunta de investigación ¿"Cómo desarrolló la Superintendencia de Industria y Comercio las facultades de inspección, vigilancia y control para garantizar el "tratamiento de datos personales" de nacionales y residentes en Colombia, durante la declaratoria de la emergencia sanitaria a causa del Coronavirus Covid – 19 mediante la Resolución 385 del 12 de marzo del año 2020 hasta el 31 de diciembre del año 2021"?

Para lograr su propósito se van a desarrollar los siguientes objetivos, siendo el general el de observar cómo desarrolló la "Superintendencia de Industria y Comercio" (Desde ahora SIC) las facultades de inspección, vigilancia y control para garantizar el "tratamiento de datos personales" de nacionales y residentes en Colombia, durante la declaratoria de la emergencia sanitaria a causa del Coronavirus Covid – 19 a partir de la resolución 385 del 12 de marzo del año 2020 hasta el 31 de diciembre del año 2021.

El primer objetivo específico es conocer el régimen de protección de datos personales en Colombia y las funciones de la SIC para proteger y garantizar el "tratamiento de datos personales" de nacionales y residentes en Colombia. El segundo es analizar las medidas adoptadas por la SIC para garantizar la "protección de los datos personales" de los ciudadanos durante la declaratoria de la emergencia sanitaria a causa del Coronavirus Covid – 19 a partir de la resolución 385 del 12 de marzo del año 2020. Y, el tercero es identificar las investigaciones y sanciones adelantadas por la SIC para la protección de datos personales desde la declaratoria de la emergencia sanitaria a causa del Coronavirus Covid – 19 a partir de la resolución 385 del 12 de marzo del año 2020 hasta el 31 de diciembre del año 2021.

Capítulo I

Régimen de Protección de Datos Personales en Colombia y las Funciones de la SIC para Proteger y Garantizar el "Tratamiento de Datos Personales" de Nacionales y Residentes en Colombia

1.1. El Derecho a la "Protección de los Datos Personales" en Colombia

El derecho fundamental al "Habeas Data", se consagró mediante el Artículo 15 de la Carta Magna, como un derecho para todos los nacionales y los residentes, y se refiere de la siguiente manera: Todas las personas colombianas o residentes, tendrán "derecho a su intimidad personal y a su buen nombre", y es deber del Estado, respetar este derecho y hacerlo respetar. Así mismo, el titular de la información tiene derecho de "conocer, actualizar y rectificar la información" que se tenga de él en bancos de datos de entidades del orden público y privado. Todo manejo que se haga de información sobre un titular de información debe ceñirse a lo preceptuado en el artículo 15 mencionado (Cote, 2016).

Esta garantía de rango constitucional es para todos y en todo sentido puesto que debe extenderse no sólo a la manifestación pública de una situación sino también a la esfera privada de cada individuo, donde debe garantizarse al máximo el respeto por la privacidad de parte del gobierno, entidad llamada a implementar medidas y procesos que salvaguarden los datos personales de los administrados (Hernández, et al., 2006. p. 149). El doctrinante Galvis (2012), señala que: La protección de datos personales, es el conjunto de normas que regulan el "tratamiento de datos personales" desde el momento en el que el receptor de la información la obtiene y luego con el posterior tratamiento que hace de la misma. Por medio de esta protección se materializa y se garantiza el derecho a la intimidad para los terceros, la libertad informática y el derecho a la información.

Al hablar de datos personales, cabe aclarar, hablamos de información que es más privada por ser de carácter exclusivo de la persona, pues esta información esta velada por un

tratamiento especial por parte de terceros sean entidades públicas o privadas, organizaciones, autoridades u otros, que deban conocerla en virtud de sus funciones o para garantizar el cumplimiento de otros derechos de superior rango constitucional y que sean de carácter general (Muñoz, 1997).

Entonces, el hecho de que el Estado, tome medidas relevantes para proteger de manera eficaz los datos personales de sus administrados, conlleva a que se disminuyan los riesgos a los cuales se ven conminadas las personas en el tratamiento de su información (Pérez, 2017). Vera, (2020) explica que bajo todas estas premisas se da trámite a la "Ley 1581 de 2012", que, además, se encuentra armonizada con el mandato constitucional del artículo 15, puesto que menciona los principios bajo los cuales se debe tratar la información privada de un tercero:

> Artículo 4. Principios para el tratamiento de datos personales:
>
> a) "Principio de legalidad en materia de tratamiento de datos": El tratamiento es una actividad regulada que debe ajustarse a la luz de la política de datos vigente a nivel estatal y otras normativas;
>
> b) "Principio de finalidad": El tratamiento debe tener un fin eminentemente legítimo de conforme a la Constitución Política y la Ley en sentido amplio, el cual debe ser informado al Titular.
>
> c) "Principio de libertad": El tratamiento de la información requiere el "consentimiento previo, expreso e informado del Titular". Se requiere este para que los "datos personales" puedan obtenerse o divulgarse, o en ausencia solo por medio de "mandato legal o judicial" pueden remplazar los debidos consentimientos.
>
> d) "Principio de veracidad o calidad": los datos sometida a los tratamientos deben ser veraces, completos, exactos, actualizados, comprobables y

comprensibles. Por ende, está prohibido aquel que posea información que se encuentre parcial, incompleto, fraccionado o que pueda inducir errores por ser falsos";

e) "Principio de transparencia": Este manejo de información se deben garantizar los derechos de los titulares para adquirirla en cualquier momento que lo necesite y sin restricción. El contenido sobre los datos que tienen almacenados, misma que debe otorgar única y exclusivamente el responsable del Tratamiento;

f) "Principio de acceso y circulación restringida": Los manejos de la información se encuentra sujeta a que se realice por parte de personas autorizadas o por las previstas en la ley con ocasión de sus funciones.

Los datos personales, no deberán estar disponibles en la red de manera pública, salvo que sea un acceso controlado con la finalidad de dar a conocer un dato de carácter general pero restringido a un público particular;

g) "Principio de seguridad": El responsable del Tratamiento de que habla la ley de habeas data y, deberá velar porque los registros que están a su cargo estén debidamente asegurados, tomando las medidas necesarias para que estos no sean adulterados, se pierdan, sean consultados por personas inescrupulosas entre otros.

h) "Principio de confidencialidad": Según la ley de habeas data, las personas que hagan parte activa en el proceso del "tratamiento de datos personales" que no posean una calidad de pública, se encuentran obligados a que se garantice la respectiva reserva, incluso si han finalizado la relación con el titular de la misma, pudiendo solamente suministrar información de estos datos cuando se deba a un mandato estipulado en la ley y que sea de obligatorio cumplimiento según lo que dice la misma (p).

Estos principios, enumerados en la "Ley 1581 de 2012", delimitan como debe realizarse el tratamiento de los datos a nivel nacional, así como entrega instrucciones sobre cómo se deben implementar políticas de "tratamiento de datos personales", para poder evitar que estos sean manipulados para cometer acciones delictivas o que puedan atentar contra el buen nombre del titular de la información, o contra su entorno personal, familiar, financiero, etc (Rojas, 2014).

Adicional a la promulgación de la "Ley 1581 de 2012", el Estado reforzó su tesis plasmada en esta ley, con la expedición del decreto 1377 de 2013, decreto que reglamentó y dio las bases para la puesta en marcha de las políticas de manejo adecuado de la información de habeas data, de que habla el artículo 15 de la carta magna, así como la expedición del Decreto 886 de 2014, para luego los dos ser compaginados en el Decreto 1074 de 2015 (Cuartas, et al., 2014). En este se incluyeron las instrucciones precisas que debe seguir el Estado y los encargados en general del "tratamiento de datos personales", al momento de inscribir información en el "Registro Nacional de Bases de Datos" (artículo 2.2.2.26.1.1. – Decreto 1074 de 2015.)

El "artículo 2.2.2.26.1.2" (Decreto 1074 de 2015). modificado por el artículo 1 del Decreto 90 de 2018, menciona en su texto que las sociedades o empresas que tengan o reporten activos iguales o superiores a 100.000 UVT, deben inscribir sus bases de datos en el "Registro Nacional de Bases de Datos", a más tardar el "día 30 de noviembre de 2018" y las "empresas que tengan activos superiores a 610.000 UVT" deben realizar dicho registro antes del 30 de septiembre de 2018. Todo esto con la finalidad de que el titular de los datos pueda ejercitar sus derechos inherentes al habeas data, cuáles sean los de "conocer, actualizar, rectificar, suprimir el/los dato(s) y/o revocar la autorización de estos" (artículo 2.2.2.26.1.4. – Decreto 1074 de 2015.)

En ese sentido se hace imperante no olvidar la "Ley 1266 de 2006", la cual es base fundamental de la legislación de hoy día y dicta aspectos generales en la materia y se regula el "manejo de la información" que está en las bases de datos financieras, crediticias y comerciales, en mayor medida (Gómez, 2015).

El “artículo 17” de la citada norma, le otorga las facultades de vigilancia a la SIC, y en lo que atañe a manejo de bases de datos de operadores, información financiera, crediticia y semejantes, a la Superintendencia Financiera.

Ahora bien, aunque todas las leyes e iniciativas sobre tratamiento y protección de datos, se promulgan buscando una cohesión entre los conceptos de cada Estado, al parecer las medidas que se están tomando no parecen ser del todo efectivas al momento de afrontar los desafíos globales, como puede ser la llegada de la era digital, pues el auge de estas plataformas donde la información personal sensible se encuentra a la orden del día y es de fácil acceso en algunos casos inclusive de grandes compañías internacionales, conlleva mayores riesgos para la privacidad y el correcto uso por parte de terceros de esta información (Cote, 2016).

El estado colombiano como garante según su función constitucional, debe tratar estos casos entendiendo que no es solo el incorrecto manejo de la información el que está en juego, sino toda la esfera de una persona en su ámbito más personal, hasta alguna información de carácter más general que de igual manera si no es bien tratada puede poner en riesgo al titular y a sus allegados (Cote, 2016).

Para ello, afirman los doctrinantes Maqueo, Moreno y Recio (2017) que el “tratamiento de los datos personales” va de la mano con otros derechos fundamentales como el de la igualdad y la no discriminación, puesto que la información de carácter sensible puede generar problemas de aislamiento o tratos que puedan considerarse discriminatorios atentando contra su persona.

Entonces el “derecho a la protección de datos personales” tiene como fin otorgar al titular de la información las herramientas y el poder para controlar la información que de su persona se recolecta, bajo el entendido y la delimitación de en qué momento se pueden intervenir por causa de alguna circunstancia que así lo requiera y cuando se puede alegar una violación sustancial al derecho aquí mencionado (Maqueo, et al, 2017).

Así con estas anteriores afirmaciones, se fortalece la postura de este derecho, como uno de naturaleza superior que precisa ser cuidado por el estado de manera primordial por cuanto hace parte del desarrollo libre de la personalidad de una persona, pues no hay mayor libertad que poder plasmar la voluntad propia escogiendo si se hace uso o no del derecho de protección que le asiste, en su faceta de información netamente hablando claro está y en lo que se refiere a los medios que la difunden y comparten información que puede afectar o no a una persona. Hay que tener en cuenta que la Pandemia de Covid- 19, trajo consigo una desmedida virtualización en todo el mundo, que obligó también a tomar medidas drásticas en materia de protección de datos personales que pueden circular rápidamente en medios virtuales (Gómez, 2020).

Esta protección, debe ser una protección en equipo, trabajo que debe ser ejecutado por las autoridades estatales encargadas de la materia, el sector privado tratante de la información y las personas que conforman la sociedad y están registrados en el sistema. "La sociedad en la cual predomina la información de un individuo, requiere más humanidad a la que se le permita y que exija sus derechos a la privacidad y la protección de datos personales" (Galvis, 2018, p. 139), así como también puede exigir la mayor efectividad de las entidades encargadas de realizar vigilancia, empezando por el adecuado uso de las TIC y el uso cada vez mayor de canales digitales (Barrera, 2020).

Ahora que se han bosquejado los conceptos importantes del "derecho a la protección" y adecuado "tratamiento de los datos personales", es necesario conocer más de la entidad encargada de supervisar y vigilar que estas políticas sean cumplidas cabalmente según el mandato imbuido a ella por la ley.

1.2. La SIC como Máxima Guardiana de los Datos Personales en Colombia

Dice entonces la "Ley 1581 de 2012" en el artículo 19, que es la SIC la responsable de realizar la vigilancia y veeduría del "tratamiento de los datos personales" en el territorio nacional, por medio de la "Delegatura para la Protección de Datos Personales", la cual vela por el respeto de los principios que menciona la ley en la materia. Adicionalmente a los

principios ya enunciados en la ley (Benavides, et al., 2019), también se han mencionado cuales son las funciones de la SIC:

Castrillón (2017) es deber de la SIC, ejercer las siguientes funciones para el adecuado cumplimiento de la ley:

a. Custodiar por la observancia de la ley en temas de habeas data,

b. Realizar las "investigaciones" necesarias, de manera oficiosa o a "petición de parte" y con base en ello ordenar lo que sea de su cargo para proteger el régimen de habeas data. Dentro de sus facultades principales está la de ordenar y conceder el acceso a la información para efectos de rectificarla, actualizarla o suprimirla;

c. Efectuar el "bloqueo temporal de los datos" cuando, aportadas la prueba necesaria por los titulares se logre vislumbrar riesgos de vulneraciones de los Derechos Fundamentales del titular y este bloqueo pueda generar una protección a estos mientras sale una decisión de fondo;

d. Implementar campañas e impartir instrucciones, dirigidas a los titulares de la información y quienes tratan la información, sobre el derecho fundamental al habeas data y su correcto ejercicio;

e. Precisar instrucciones puntuales sobre las medidas necesarias para la adecuación de las operaciones de quienes tratan esta información;

f. Solicitar a los encargados del tratamiento de la información la información necesaria para efectivizar sus funciones entre otras que son de obligatorio cumplimiento para la realización del deber de la Superintendencia y de quienes se encuentran dentro del proceso de tratamiento de datos (art.21).

Es evidente, que la SIC fue investida de herramientas reforzadas para evitar vulneración al régimen de "tratamiento de datos personales" en Colombia, puesto que además de velar por el cumplimiento de la ley, le son atribuidas funciones judiciales en la materia, por ser la entidad que encabeza el conocimiento de la materia, siendo órgano de cierre de primera instancia inclusive (Benavides, 2019).

Con el fin de facilitar sus funciones, en materia de transparencia, la SIC ha diseñado un juicioso ejercicio de funciones y Políticas que se encuentran alineadas con la normatividad precedente, pues tiene unos principios rectores que se asemejan a lo instituido hoy día, a saber:

> i) Principio de legalidad en materia de datos personales; ii) Principio de finalidad; iii) Principio de libertad; iv) Principio de veracidad o calidad; v) Principio de transparencia; vi) Principio de acceso y circulación restringida; vii) Principio de seguridad; viii) Principio de confidencialidad; ix) Principio de temporalidad; x) Principio de interpretación integral de los derechos constitucionales; xi) Principio de necesidad (SIC, s.f., p.1).

Teniendo en cuenta su calidad de órgano vigilante, también le compete a la SIC generar conceptos y doctrina que permita allanar el camino sobre el tema que nos compete, en especial en lo que respecta a la diligencia que deben emplear los responsables de la información y les conmina a acatar las disposiciones en la materia (González, 2018). Básicamente la entidad precisa que la administración correcta de datos requiere también garantizar la seguridad de estos. Así pues, el tratamiento de datos que no se encuentre acorde, no debe ser considerado legal (Resolución 1321 del 2019).

En cuanto al punto anteriormente mencionado, sobre la masificación de las herramientas virtuales debido al Covid- 19, la SIC como garante de este derecho en nombre del Estado ha estado atenta a proveer lo necesario para proteger los datos de las personas y velar porque las personas se atengan a lo citado en la ley (Peña, et al., 2022). Por esto a través de la "Delegatura para la Protección de Datos Personales" (SIC), ha sacado guías con carácter

de recomendación, para los "titulares de la información y los responsables del trato de la misma". Unas de las guías más importantes que ha sacado y ayudan al público no conocedor a empaparse del tema, son:

> Guía cuida tu identidad digital y protege tus datos personales: riesgos sobre el tratamiento de datos personales de niños, niñas y adolescentes; Guía para recomendaciones para el tratamiento de datos personales mediante el servicio de computación en la nube; Recomendaciones generales para el tratamiento de datos en inteligencia artificial; Asuntos prácticos sobre el Derecho de Habeas Data; Guía sobre tratamiento de datos personales para fines de marketing y publicidad; Guía para solicitar la declaración de conformidad en transferencias internacionales de datos personales; Guía de datos personales para fines de comercio electrónico (SIC, s.f, p.1).

Básicamente estas guías se formaron para minimizar o erradicar con la implementación de estas guías, específicamente los siguientes incidentes de seguridad muy comunes y que representan gran cantidad de litigios y denuncias (Cote, 2016):

I "Riesgos en la seguridad física o psicológica", II "Extorsión económica o sexual" III "Hurto de identidad", IV "Suplantación de identidad", V "Perdida financiera", VI "Negación de un crédito o seguro", VII "Perfilamiento con fines ilícitos", VIII "Perdidas de negocio y/o oportunidades de empleo", IX "Discriminación", y X "Humillación significativa o perdida de dignidad y daño a la reputación"

Lo interesante es que la SIC no se ha circunscrito a sí misma a una función de carácter meramente administrativo, ya que, en varios de sus conceptos y pronunciamientos en la materia, ha sentado precedentes jurisprudenciales sobre los derechos que se deben tener como primordiales en materia de datos personales (Estrada, 2014).

Capítulo II

Analizar las Medidas Adoptadas por la Sic para Garantizar la Protección de los Datos Personales de los Ciudadanos Durante la Declaratoria de la Emergencia Sanitaria a Causa del Coronavirus Covid – 19 a partir de la Resolución 385 del 12 de Marzo del Año 2020

Como se precisa anteriormente, la contingencia y los procesos surgidos de la pandemia del Covid-19, puso en riesgo inminente muchas instituciones y a toda la humanidad en cuanto a salud nos referimos. Producto de las instrucciones para salvaguardar este derecho a la salud, muchas situaciones que precisaban interacción entre personas, rápidamente debieron ser intervenidas para reemplazarlas y poder tener una vida medianamente normal dentro de lo que cabía (Gómez, 2020).

Las medidas iniciales, buscaban a toda costa, disminuir a su mínima expresión el contacto entre personas y por ello mediante la "Resolución 12169 de 2020" procedió a reglamentar un documento formal, reglamentación que iba encajada con lo indicado dentro de la Resolución No. 385 del 12 de Marzo de 2020 por medio de la cual se declaró la "emergencia sanitaria por el Ministerio de Salud y Protección Social" y se resuelve suspender los términos de las "actuaciones administrativas" de carácter sancionatorio y disciplinarias en curso, desde el 17 de abril de 2020 y hasta la duración del aislamiento preventivo decretado por el Presidente de la República con la coadyuvancia del "Ministerio de Salud y de la Protección Social" (Gómez, 2020).

Gómez (2020) explica que como se puede ver, en el parágrafo primero de la resolución se indica que no es posible suspender términos en procesos administrativos en los que se traten derechos fundamentales, específicamente aquellos atenientes a la protección del derecho al habeas data, protección al consumidor entre otros de semejante índole.

El parágrafo primero de la resolución en cita sostiene que no se puede aplicar la suspensión de términos en los procesos administrativos en los cuales se toquen el cumplimiento y "efectividad de derechos fundamentales" en especial aquellos concernientes a las garantías sobre el "habeas data", "protección al consumidor", prácticas restrictivas de la competencia y de aquellas que consideren indispensable para solventar la "crisis causada por el coronavirus COVID – 19".

En este primer pronunciamiento de la entidad, se realizó un concepto muy general de cómo se llevarían a cabo las actuaciones administrativas de la entidad, sin entrar en mayores detalles. Pero cuando las herramientas digitales se pusieron a la orden del día, la SIC adquirió un rol fuerte y sumamente importante, siendo mediante sus directrices, garante de la información personal de las personas en sus videos llamadas y demás herramientas de conexión, lo que se vio por la cantidad de circulares externas que emitió durante la duración de la emergencia sanitaria decretada.

La primera Resolución de la SIC, fue dirigida a los operadores de telefonía móvil, donde se les indicaba como debían suministrar información al DNP y a las entidades que requirieran los datos de los usuarios, con la finalidad de tratarlos, atenderlos y prevenir contagios y la propagación del brote. En efecto la SIC manifestó que:

Conforme lo dispuesto en el "literal c) del Artículo 10 de la Ley Estatutaria 1581 del 2012", no será necesaria la autorización del titular para poder tratar los datos, cuando se requiera su uso por una emergencia médica. El literal b) del artículo 13 por otro lado, ordena que los datos podrán ser entregados a las entidades públicas o administrativas que por razón de sus funciones las requieran para tratar o prevenir la propagación del Covid-19. Así mismo se menciona la obligatoriedad de guardar esta información con carácter de reserva.

También se hacía el llamado a las entidades de telefonía, para facilitar la entrega de números telefónicos de contacto de las personas de la base de datos del SISBÉN, para poder entregar un insumo valioso a las entidades médicas encargadas de trabajar con población

vulnerable adscrita a este régimen especial, pero siempre teniendo en cuenta las medidas de seguridad de la información, para evitar suplantaciones y demás.

Por medio de la "Circular Externa 002 de 27 de marzo de 2020", la SIC recomendó no usar huelleros para recolección de información de datos biométricos, esto buscando prevenir contagios por posible contacto, siendo también precursora de políticas de salud públicas. Así, dijo:

> A los responsables y encargados del tratamiento de la información, que sean de naturaleza pública o privada, se sirvan abstenerse de recolectar o tratar datos biométricos utilizando huelleros físicos o electrónicos, ya que puede incitar el contagio del coronavirus a través de contacto indirecto. Esta instrucción no aplica para el caso de los sistemas de identificación biométrica en los que el dispositivo sea personal e individual. Esta orden es de inmediata ejecución, tienen carácter preventivo, obligatorio y aplica sin perjuicio de las instrucciones que emitan otras autoridades en el marco de sus atribuciones constitucionales y legales (SIC, 2020, p.1).

Este último sirvió para probar ejemplos y protocolos de bioseguridad de otros países de la zona y también para poner a la entidad como referente de valiosos aportes a la salud pública y manteniendo fidelidad a su deber de guarda de los datos personales de los administrados (Peña, 2022).

Trujillo (2021) mediante la Circular Externa No. 008 de 2020, la SIC entregó las siguientes recomendaciones sobre recolección y trato de datos para cumplir con "protocolos de bioseguridad": SEGUNDO: RECOLECCIÓN DE DATOS. Hay que tener presente que:

> a) No se pueden engañar o inducir a fraude para "recolectar y realizar tratamiento de datos personales" (Ley 1581 de 2012).

b) Se debe informar al titular de la información cuál es la "finalidad específica de la recolección de sus datos" (Ley 1581 de 2012).

c) "No se puede recolectar cualquier dato sino solo aquel o aquellos que sean pertinentes para la finalidad por la cual se solicita. Los responsables del tratamiento de datos personales deben estar en capacidad de justificar o explicar la necesidad de recolectar los datos que solicitan a las personas sin perjuicio alguno" (Ley 1581 de 2012).

d) "No se deben recolectar datos diferentes a los exigidos expresamente por el Ministerio de Salud y Protección Social para efectos de dar cumplimiento a los protocolos" (Ley 1581 de 2012).

e) "Salvo en los casos previstos en la ley, no se podrán recolectar datos personales sin contar con la autorización del Titular. La autorización se podrá obtener por los mecanismos previstos en el Artículo 7 del Decreto 1377 de 2013, pero es el responsable de su tratamiento quién tiene el deber de conservar prueba de dicho consentimiento para los efectos pertinentes" (Ley 1581 de 2012) (p. 24).

Como en todo, hubo quienes no estuvieron de acuerdo con algunas de las decisiones de la SIC en cuanto manifiestan que se alejó de su norte y de su papel de garante de los datos personales de los administrados, no obstante lo cual este reproche se invalida con el concepto de la SIC, ya que esta circunscribió la recolección de datos de manera única a las necesidades del Ministerio de Salud, lo que garantizaba que los datos que fueran sensibles pero no necesarios, se conservarían o se presume, se debían conservar intactos pues solo debían usarse aquellos cuyo fin era evitar la propagación del Covid- 19 (Corredor, 2020).

También en la Circular Externa, la SIC fue tajante en su exigencia de precisar protocolos idóneos para cumplir con un correcto tratamiento de la información: cuarto: seguridad y confidencialidad de los datos, donde se debe hacer uso de las medidas necesarias

para garantizar la seguridad de los datos personales, evitando que sean adulterados, se pierdan o sean consultados por personas inescrupulosas (Trujillo, 2021).

Durante la duración del estado de emergencia sanitaria, se conocieron circulares externas de dicha entidad donde esta entregaba al público, medidas para un correcto manejo de la información durante el trascurso de la pandemia y hasta tanto esta no estuviera controlada. Luego, a manera recopilatoria, mediante la expedición de la Circular única, se incluyeron varias de las normativas dictadas hasta ese momento, pero no todas, proporcionando con esto a los terceros interesados y los funcionarios, un instrumento legal con unas reglas determinadas a tener presentes (Peña, 2022).

Ahora bien, preciso es indicar que la circular única enfatiza las directrices sobre recolección, manejo, tratamiento y transferencia de datos personales para efectos de "información financiera, crediticia, comercial, de servicios", situaciones que se regulan bajo la expedición de la normativa de la Ley 1266 de 2008 (Gómez, 2020), la cual se divide en: "Capítulo I: Derecho de Habeas Data para información financiera, crediticia, comercial, de servicios y la proveniente de terceros países; Capítulo II: Registro Nacional de Base de Datos-RNBD; Capítulo III: Transferencia de Datos Personales a terceros países" (SIC, s.f).

La SIC hasta el momento no ha realizado la recopilación de todas las reglamentaciones e instrucciones en el manejo de datos personales regulado bajo la "Ley 1581 de 2012".

El capítulo I de la Circular Única expedida en mayo del 2020, tiene como premisa esencial la de dar a conocer a los particulares y los tratantes de la información, cuáles son las pautas y los procedimientos a tener en cuenta de parte de los operadores, las fuentes y los usuarios de información financiera (Gómez, 2020).

Capítulo III

Investigaciones y Sanciones Adelantadas por la Superintendencia de Industria y Comercio para la Protección de Datos Personales desde la Declaratoria de la Emergencia Sanitaria a Causa del Coronavirus Covid – 19 a partir de la Resolución 385 del 12 de marzo del Año 2020 hasta el 31 de diciembre del Año 2021

Se estudiará la totalidad de las resoluciones proferidas por la Dirección de protección de datos personales, en el marco de la declaración de estado de emergencia sanitaria por la pandemia del Sars-Covid 19. Se analiza las resoluciones a partir de la Resolución 385 de 2020 hasta el 31 de diciembre de 2021, buscando conocer que actuaciones o hechos cometidos podrían afectar o alterar la seguridad de los datos personales de nacionales y residentes en Colombia, así como los argumentos usados para expedir y sancionar estas disposiciones que iban en conjunto con la disposición de la ley 1581 de 2012, ley de protección de datos personales.

La Ley 79 de 1993 por la cual se regula la realización de los censos de población y vivienda en todo el territorio nacional, promulga en su artículo 5 que:

> Las personas naturales o jurídicas, de cualquier orden o naturaleza, domiciliadas o residentes en el territorio nacional, están obligadas a suministrar al Departamento Administrativo Nacional de Estadística D.A.N.E, los datos solicitados en el desarrollo de Censos y Encuestas. Los datos suministrados al Departamento Administrativo Nacional de Estadística DANE, en el desarrollo de los censos y encuestas, no podrán darse a conocer al público ni a las entidades u organismos oficiales, ni a las autoridades públicas, sino únicamente en resúmenes numéricos, que no hagan posible deducir de ellos información alguna de carácter individual que pudiera

> utilizarse para fines comerciales, de tributación fiscal, de investigación judicial o cualquier otro diferente del propiamente estadístico (p).

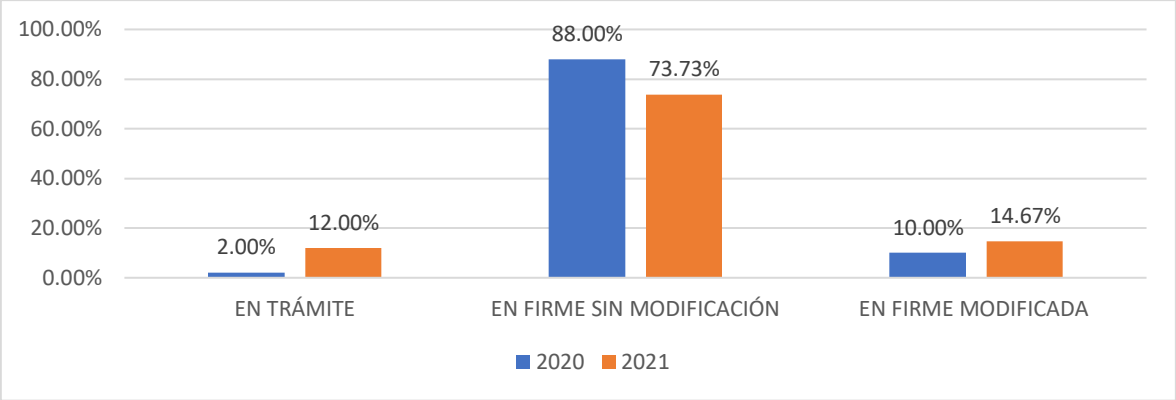
De acuerdo a lo anterior, la SIC también se ampara bajo esta ley que refiere a la protección de datos personales, y que por efectos de las encuestas realizadas por el DANE, la información suministrada por los encuestados, ya sean personas jurídicas o naturales, no se dará a conocer al público como tampoco a las entidades u organismos oficiales, entre ellas la SIC.

De esta manera se da inicio en el año 2020, donde la SIC facultada como entidad protectora de los datos personales, profirió cincuenta Resoluciones, de las que solo algunas contadas fueron por investigaciones adelantadas oficiosamente. Así mismo, solo el 2% se encuentra en trámite, se desconocen las circunstancias que motivan a que este proceso no se haya culminado. Por su parte el 88% de las Resoluciones se encuentran en firme y sin ninguna modificación, y el 10% de las Resoluciones se encuentran en firme y fueron modificadas en instancia de reposición, para un total de 98% de la Resoluciones están ejecutoriadas.

Para el año 2021, donde la SIC facultada como entidad protectora de los datos personales, profirió ochenta y siete Resoluciones. Dentro de las cuales el 9% aún se encuentran en trámite. Por su parte, el 73% de las Resoluciones están en firme y no poseen ninguna modificación, y el 14,67% de las Resoluciones se encuentran en firme y fueron modificadas en instancia de reposición, para un total del 88% de las Resoluciones están ejecutoriadas.

En términos porcentuales podemos evidenciar la siguiente gráfica:

Gráfica 1. ***Porcentaje del Estado del Trámite de las Resoluciones***



Nota. Elaboración propia.

En esta gráfica se puede observar que el 98% en 2020 y el 88% para el 2021 de los casos fueron resueltos y se encuentran ejecutoriados en la actualidad, de estos tan solo el 10% fueron modificados en segunda instancia en el 2020 y 14,67% en 2021. Por ende, se evidencia un alto índice de eficacia en brindar justicia dentro de la función jurisdiccional que presta la SIC, pues tan solo el 2% de los casos se encuentran abiertos y sin una respuesta definitiva en el año 2020 y el 12% en 2021; valor porcentual minúsculo para el primer año y aún mayor en el segundo, pero este incremento solo obedece a que solo ha transcurrido un año desde entonces. En este punto, es importante realizar una nota distintiva con la jurisdicción ordinaria, pues esta se caracteriza por la lentitud de sus procesos y por la demora en brindar justicia a los ciudadanos. Es así, como Superintendencia de Industria y Comercio en asuntos jurisdiccionales en esta temática es más expedita que la jurisdicción ordinaria. Este factor puede deberse a dos importantes factores como son la sistematización de los procesos y el conocimiento especializados de quién funge como juez por parte de la SIC. En cuanto en resumen los principales criterios de las sanciones dada de manera conjunta que se puede

encontrar en las Resoluciones de los dos años se pueden encontrar a continuación. En un porcentaje de 2% y 1,33% para el 2020 y 2021 respectivamente, que equivalen los porcentajes a una sola Resolución, se evidencian los siguientes criterios:

Resoluciones 2020	**Resoluciones 2021**
1. Dimensión del daño o peligro para los intereses jurídicos tutelados por la ley. 2. Reincidencia en la comisión de la Infracción	1. Dimensión del daño o peligro para los intereses jurídicos tutelados por la ley. 2. Reincidencia en la comisión de la Infracción
1. Dimensión del daño o peligro para los intereses jurídicos tutelados por la ley. 2. Reconocimiento o aceptación de la comisión de una infracción. 3. Reincidencia en la comisión de la Infracción	1. Dimensión del daño o peligro para los intereses jurídicos tutelados por la ley. 2. 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. 3. La reincidencia en la comisión de la infracción.

Se pueden encontrar en el 4% en el 2020 y 69,33% en el 2021 de las Resoluciones el siguiente criterio:

1) "1. Dimensión del daño o peligro para los intereses jurídicos tutelados por la ley. 2. Aplicación del principio de Responsabilidad demostrada" (SIC, 2020, p. 1).

Por su parte en un nivel mayor en el 20% en el 2020 y 2,67% en el 2021 de las Resoluciones se puede observar las siguiente:

2) "Dimensión del daño o peligro para los intereses jurídicos tutelados por la ley. 2. Reconocimiento o aceptación de la comisión de una infracción" (SIC, 2020, p. 1).

En un total del 60% en el 2020 y 69,33% en el 2021 de las Resoluciones se evidencia solo el siguiente:

3) "Dimensión del daño o peligro para los intereses jurídicos tutelados por la ley" (SIC, 2020, p. 1).

En cuanto a los criterios que se localizan sin su equivalente en el otro año se encuentran para el 2021:

En un porcentaje de 2,67% de las Resoluciones del 2021:

4) “1. Dimensión del daño o peligro para los intereses jurídicos tutelados por la ley. 2. Reincidencia en la comisión de la Infracción” (SIC, 2020, p. 1).
5) “1. El deber de los responsables del Tratamiento de cumplir las instrucciones. 2. y requerimientos que imparta esta Superintendencia” (SIC, 2020, p. 1).
6) “1. Obligación de cumplir con la ley colombiana 2. Respeto por las leyes en el ciberespacio 3. Riesgo para los derechos y libertades de las personas frente al tratamiento de sus datos personales. 4. Deber de conservar la información de los usuarios segura. 5. Formas de tratamiento de datos llevadas a cabo por Zoom. 6. Hallazgos de análisis técnico y respuesta de Zoom (Hurto de credenciales, transferencia de información de Zoom a Facebook, acceso a perfiles de Linkedin” (SIC, 2020, p. 1).

En un porcentaje de 8% de las Resoluciones del 2021:

7) “Renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio” (SIC, 2020, p. 1).

Los criterios que solo se encuentran una vez para el año 2020:

“1. Criterios de la Resolución 53593 de 2020 por medio de la cual se imparten instrucciones a Google LLC para que garantice el tratamiento de datos personales conforme lo dispone la Ley 1581 de 2012. 2, Análisis de la relación jurídica y societaria de Google LLC con Google Colombia Limitada. 3. Google LLC y Google Colombia Limitada actúan en concurso y tienen la ibligación de cumplir con la legislación colombiana en materia de tratamiento de datos personales de terceros. 4. Tratamiento de datos personales de niños, niñas y adolescentes de parte de Google. 5. Primacía de la realidad sobre las formas. 6. El uso de la marca Google relaciona a ambas sociedades

entre sí y les otorga la responsabilidad compartida de tratar cuidadosamente la información recibida" (SIC, 2020, p. 1).

"1. Deber de garantizar al titular de la información, el ejercicio pleno de su derecho constitucional al Habeas Data" (SIC, 2020, p. 1).

"1. Deber de solicitar y conservar en las condiciones previstas en la ley, copia de la autorización de tratamiento de datos otorgada por el titular. 2. Deber de garantizar al titular de la información, el ejercicio pleno de su derecho constitucional al Habeas Data. 3. Aplicación del principio de Responsabilidad demostrada" (SIC, 2020, p. 1).

"1. La ley 1581 de 2012 es aplicable a ByteDance Ltd., TikTok Inc. y Tik Tok Pte. Ltda ya que mediante la aplicación TikTok recolectan información de datos personales a través de Cookies. 2. ByteDance Ltd y las mencionadas empresas tienen la obligación de cumplir la legislación colombiana. 3. Las leyes en el ciberespacio deben ser respetadas. 4. TikTok no tiene políticas de privaciad en español para sus usuarios en Colombia. 5. Tratamiento de datos personales de niñas, niños y adolescentes" (SIC, 2020, p. 1).

"1. Obligación de cumplir con la ley colombiana 2. Respeto por las leyes en el ciberespacio 3. Riesgo para los derechos y libertades de las personas frente al tratamiento de sus datos personales. 4. Deber de conservar la información de los usuarios segura" (SIC, 2020, p. 1).

"1. Servicios que ofrece Google LLC. 2. La ley 1581 de 2012 es aplicable a Google LLC ya que recolecta información y datos personales en el territorio colombiano. 3. Google LLC tiene la obligación de cumplir la legislación colombiana, así como las órdenes y requerimientos de esta autoridad, en cumplimiento de la Ley 1581 de 2012. 4. Google reconoce que el tratamiento de datos personales está sujeto a la legislación aplicable en el país donde se realiza dicho tratamiento. 5. La forma en la cual Google realiza el tratamiento de datos personales. 6. Tratamiento de datos personales por parte de Google de niños, niñas y adolescentes. 7. Debida diligencia en el tratamiento de información de

niñas, niños y adolescentes. 8. Actuaciones y decisiones de autoridades extranjeras sobre el consentimiento previo del representante legal para realizar el tratamiento de datos de niños, niñas y adolescentes. 9. Cumplimiento del artículo 12 de la ley 1581 de 2012. 10. Cumplimiento por parte de Google de los requisitos que debe tener la política de tratamiento de la información" (SIC, 2020, p. 1).

Finalmente, los criterios que solo se encuentran una vez para el año 2020:

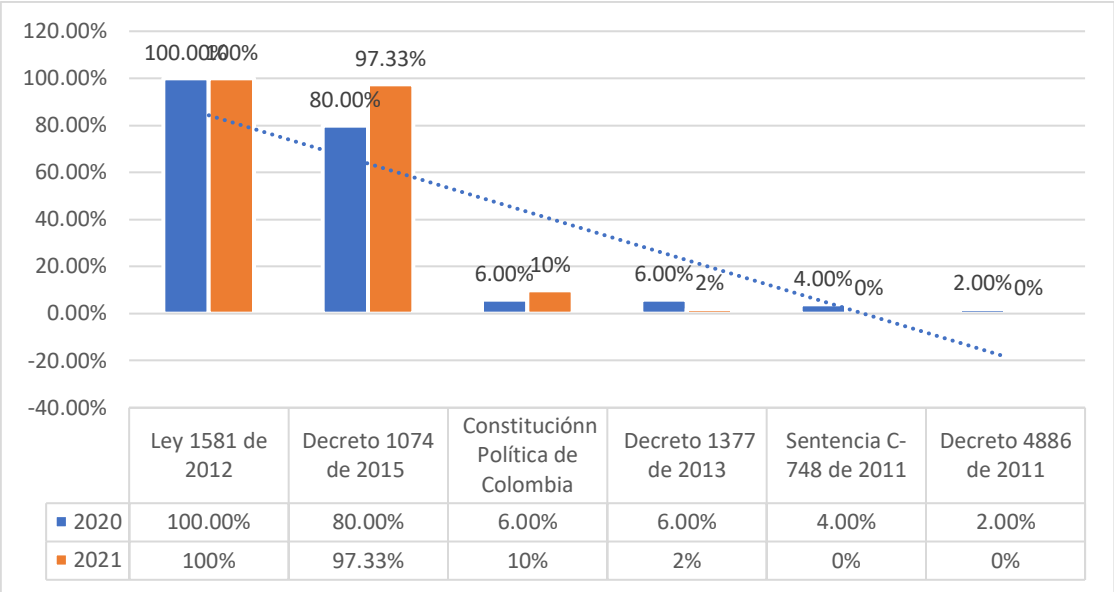
"1. Dimensión del daño o peligro para los intereses jurídicos tutelados por la ley. 2. Renuencia o desacato a cumplir las órdenes e instrucciones impartidas por la Superintendencia de Industria y Comercio" (SIC, 2020, p. 1).

"1. Suspensión de las actividades del banco de datos hasta por un término de seis (6) meses. Artículo 18 de la Ley 1266 de 2008. 2 suspensión de las actividades relacionadas con el Tratamiento hasta por un término de tres (3) meses" (SIC, 2020, p. 1).

Entre los principales fundamentos normativos encontramos para el 2020 y 2021:

El porcentaje de manera gráfica se puede observar lo siguiente:

Gráfica 2. ***Porcentaje del fundamento normativo***



	Ley 1581 de 2012	Decreto 1074 de 2015	Constitucionn Política de Colombia	Decreto 1377 de 2013	Sentencia C-748 de 2011	Decreto 4886 de 2011
2020	100.00%	80.00%	6.00%	6.00%	4.00%	2.00%
2021	100%	97.33%	10%	2%	0%	0%

Nota. Elaboración propia.

Es así como se evidencia que la principal fuente normativa de las Resoluciones obedece a su misma naturaleza como es la Ley 1581 de 2012 “Ley de Protección de Datos Personales” con un porcentaje del 100%., es decir, la totalidad de las Resoluciones emplean esta fuente par ambos años. Seguido en una menor medida por el Decreto “Decreto Único Reglamentario del Sector Comercio, Industria y Turismo” con un 80% para el 2020 y el 97,33% para el 2021. Después sigue los fundamentos constitucionales con el 6% para el 2020 y el 10% para el 2021 y el Decreto 1377 de 2013 “Por el cual se reglamenta parcialmente la Ley 1581 de 2012, Derogado Parcialmente por el Decreto 1081 de 2015” con el mismo 6% para el 2020 y el 2% para el 2021.

A continuación, de manera exclusiva para el año 2020 la Sentencia C- 748 de 2011, mediante la cual se evalúa de manera oficiosa por parte de la Corte Constitucional la constitucionalidad de la Ley Estatutaria sobre protección de datos, con un 4% y finalmente, el Decreto 4886 de 2011 “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” con un 2%.

En cuanto al principal Derecho vulnerado se encuentra el "habeas data", del total del 100% de las Resoluciones en 92% para el 2020 y el 97,33% para el 2021 se sancionó a la persona natural o jurídica investigada por este concepto. Y cuando este no ha sido aún afectado y se encuentra en riesgo, las Resoluciones emiten una orden preventiva las cuales corresponden a solo el 8% para el 2020 y el 2,67% para el 2021 de las emitidas desde marzo a diciembre de 2020.

Entre las ordenes preventiva del 2020 encontramos las siguientes:

- "Ordenar a Zoom tomar medidas para adecuar sus operaciones a la legislación colombiana" (SIC, 2020, p. 1).
- Sanción a la constructora Amarilo S.A.S. por presunta violación de las normas sobre protección de datos personales y, en particular, las disposiciones contenidas el 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, y el artículo 2.2.2.25.2.2 del Decreto Único Reglamentario 1074 de 2015, se inició la presente investigación administrativa mediante la expedición de la Resolución No. 34218 de 6 de agosto de 2019, por medio de la cual se formuló un único cargo a la sociedad AMARILO S.A.S.

- Ordenar a ByteDance Ltd., TikTok Inc. y TikTok Pte. Ltd.
    - "Implementar mecanismos apropiados y efectivos en el momento en el cual solicitan información o autorización al titular de la información. Dicha información deberá estar en español" (SIC, 2020, p. 1).
    - "Dar aplicación tácita al artículo 12 de la Ley 1581 de 2012 en lo referente al manejo y cuidado de la información de niños, niñas y adolescentes en la República de Colombia" (SIC, 2020, p. 1).

- De manera concreta a TikTok
    - "Crear una política de tratamiento de datos congruente a la legislación colombiana y en idioma español, cumpliendo con lo dispuesto en el artículo

13 del Decreto 1377 de 2013, colocando a disposición de los titulares de la información dicha política adoptada" (SIC, 2020, p. 1).

- "Que sobre los datos personales recolectados y que sean de menores de edad, provean a la Superintendencia los permisos o autorizaciones de sus tutores o representantes legales para ello" (SIC, 2020, p. 1).
- "Deberá remitir un informe realizado por una empresa imparcial y ajena a los intereses de la investigada, en el cual manifieste el cumplimiento de lo dicho en el Decreto, el número de autorizaciones con que cuenta desde que entró en vigencia la ley 1581 de 2012 y que dichas autorizaciones cumplan con los parámetros y requisitos impuestos por la ley para su validez" (SIC, 2020, p. 1).

- Ordenar a Google LLC:
  - "Implementar un mecanismo idóneo sobre el tratamiento de datos personales de nacionales colombianos o residentes, para que al momento de solicitar información se cumpla con lo dispuesto en la ley 1581 de 2012" (SIC, 2020, p. 1).
  - "Crear una política de tratamiento de datos personales acorde con la legislación vigente en especial lo dispuesto en el artículo 13 del Decreto 1377 de 2013 así como ponerla al alcance de los titulares de la información" (SIC, 2020, p. 1).
  - "Implementar un mecanismo eficiente que cumpla con los estándares y lo dispuesto en el artículo 12 del decreto 1377 de 2013" (SIC, 2020, p. 1).
  - "Respecto de los datos recolectados de personas nacionales o residentes en Colombia, registrar sus bases de datos en el Registro Nacional de Bases de Datos de la SIC" (SIC, 2020, p. 1).
  - "Sobre los datos que administra, suministre a la SIC las autorizaciones previas de los representantes legales de los menores de edad cuyos datos hayan sido recolectados o tratados posteriores a la vigencia de la ley 1581 de 2012" (SIC, 2020, p. 1).

- “Presentar las correcciones solicitados dentro del mes siguiente a la ejecutoria de la Resolución, informe que deberá ser presentado por un tercero sin intereses contrapuestos” (SIC, 2020, p. 1).

En el caso de TikTok, esta fue una determinación relevante y novedosa por parte de la Superintendencia, pues fue una alerta a TikTok para moverse un poco más allá de lo escrito en el papel y tomar verdaderas medidas que garantizaran la seguridad de los usuarios también en el ambiente virtual de la plataforma. Así entonces, le pidió la SIC a la app, implementar un método eficaz y probable al momento de pedir la autorización de tratamiento de datos por parte del titular, para garantizar el adecuado y seguro tratamiento de sus datos. También exigió que la información de la cual eran tratantes fuera inscrita en el RNBD.

Donde la SIC indica que por la manera particular en la cual se gesta la relación entre el usuario y la plataforma la responsabilidad de la empresa sobre la protección de los datos no es de carácter renunciable puesto que, aunque se trata de la relación entre usuario y empresa en un espacio virtual, este espacio no tiene unas reglas y unas fronteras clarificadas. En este mundo digital, confluyen diariamente millones de personas de varias partes del mundo, pero, aunque el sitio de aglutinamiento sea una realidad virtual, lo cierto es que estos actos se ejecutan desde nuestra realidad, y los actos ejecutados desde esta realidad tienen consecuencias positivas o negativas según sea el caso.

Entre las ordenes preventiva del 2021 encontramos las siguientes:

- Ordenar a la ALCALDÍA MAYOR DEL DISTRITO DE BOGOTÁ D.C que:
  - “Proceda a implementar mecanismos oportunos, útiles, necesarios, eficientes, eficaces y demostrables que fortalezcan las medidas de seguridad, confidencialidad, uso limitado, acceso y circulación restringida de los datos personales, en especial, los de naturaleza sensible que se encuentran en el aplicativo PAI 2.0, así como en cualquier otro desarrollo tecnológico o de otra índole que se pretenda implementar o que se esté implementando en el que se realice Tratamiento de Datos Personales” (SIC, 2020, p. 1).

- “Procedan a la implementación efectiva e inmediata del Principio de Responsabilidad Demostrada” (SIC, 2020, p. 1).

- “Abstenerse de poner en funcionamiento sistemas de información en internet u otros medios de divulgación y comunicación masiva que contengan datos personales privados, semiprivados o sensibles sin que previamente haya verificado que existen procesos, mecanismos, herramientas y controles técnicos o de cualquier otra naturaleza que sean pertinentes, efectivos y útiles para brindar un conocimiento o acceso restringido sólo a los Titulares de los datos personales o terceros autorizados conforme a lo señalado en la Ley Estatutaria 1581 de 2012” (SIC, 2020, p. 1).

- Ordenar a la sociedad WhatsApp LLC (en adelante WhatsApp) que:
  - “Respecto de los Datos personales que recolectan o tratan en el territorio de la República de Colombia sobre personas residentes o domiciliadas en este país, implementen un mecanismo o procedimiento apropiado, efectivo y demostrable para que, al momento de solicitar la Autorización al Titular, le informen en idioma castellano, de manera clara, sencilla y expresa todo lo que ordena el artículo 12 de la Ley Estatutaria 1581 de 2012” (SIC, 2020, p. 1).

  - “Crear una Política de Tratamiento de Información (PTI) redactada en idioma castellano y que cumpla todos los requisitos que exige el artículo 13 del Decreto 1377 de 2013 (incorporado en el artículo 2.2.2.25.3.1 del Decreto 1074 de 2015). Dicha PTI debe ser puesta en conocimiento de los Titulares de los Datos domiciliados” (SIC, 2020, p. 1).

  - “Respecto de los Datos que recolectan o tratan en el territorio de la República de Colombia sobre personas residentes o domiciliadas en este país, registren sus Bases de Datos en el Registro Nacional de Bases de Datos (RNBD),

administrado por la Superintendencia de Industria y Comercio" (SIC, 2020, p. 1).

Se puede ver que la SIC despliega todas sus herramientas, definidas en cada una de sus delegaturas, ejerciendo su función de ente controlador en el examen que realiza del documento presentado por la Secretaría Distrital de Salud, llamado "Análisis Técnico", en el cual no encuentra cumplidas las medidas necesarias para garantizar la seguridad de los datos de las personas que ingresan al aplicativo.

Conclusiones

El presente trabajo para dar respuesta a la pregunta de investigación de ¿"Cómo desarrolló la Superintendencia de Industria y Comercio las facultades de inspección, vigilancia y control para garantizar el "tratamiento de datos personales" de nacionales y residentes en Colombia, durante la declaratoria de la emergencia sanitaria a causa del Coronavirus Covid – 19 mediante la Resolución 385 del 12 de marzo del año 2020 hasta el 31 de diciembre del año 2021"?

Realizó un análisis dogmático y abordó de manera integral y exhaustiva las facultades de inspección, vigilancia y control dadas a la SIC como entidad responsable de garantizar el tratamiento de datos personales de nacionales y residentes en Colombia, para lo cual examinó y analizó el régimen de protección datos personales en Colombia, las funciones de la SIC para proteger y garantizar el "tratamiento de datos personales" de nacionales y residentes en Colombia, las medidas adoptadas por la SIC para garantizar la protección de

los datos personales de los ciudadanos durante la declaratoria de la emergencia sanitaria a causa del coronavirus COVID – 19 a partir de la resolución 385 del 12 de marzo del año 2020 e investigaciones y sanciones adelantadas por la Superintendencia de Industria y Comercio para la protección de datos personales desde la declaratoria de la emergencia sanitaria a causa del coronavirus COVID – 19 a partir de la resolución 385 del 12 de marzo del año 2020 hasta el 31 de diciembre del año 2021.

En conclusión, los datos personales en Colombia es un derecho fundamental consagrado en el artículo 15 de la constitución política colombiana, derecho reglamentado en la Ley 1581 del año 2012.

Adicional a la promulgación de la "Ley 1581 de 2012", el Estado reforzó su tesis plasmada en esta ley, con la expedición del decreto 1377 de 2013, decreto que reglamentó y dio las bases para la puesta en marcha de las políticas de manejo adecuado de la información de habeas data, de que habla el artículo 15 de la carta magna, así como la expedición del Decreto 886 de 2014, para luego los dos ser compaginados en el Decreto 1074 de 2015 (Cuartas, et al., 2014). En este se incluyeron las instrucciones precisas que debe seguir el Estado y los encargados en general del "tratamiento de datos personales", al momento de inscribir información en el "Registro Nacional de Bases de Datos"

La Superintendencia de Industria y Comercio – SIC, por mandato del artículo 19 de la Ley 1581 del año 2012, es la responsable de realizar la vigilancia y veeduría del "tratamiento de los datos personales" en el territorio nacional, por medio de la "Delegatura para la Protección de Datos Personales", la cual vela por el respeto de los principios que menciona la ley en la materia.

El artículo 21 de la Ley 1581 del 2012, otorga a la SIC las funciones de velar por el cumplimiento de la legislación en materia de protección de datos personales, adelantar investigaciones de oficio o a petición de parte, disponer el bloqueo temporal de los datos cuando se identifique un riesgo de vulneración de los derechos fundamentales, promover y divulgar los derechos sobre el tratamiento de datos personales, impartir instrucciones sobre

las medidas y procedimientos en las operaciones de los responsables del tratamiento, solicitar al responsable información necesaria para el ejercicio de sus funciones, sugerir o recomendar los ajustes o adecuaciones a la normatividad que le sean acordes y requerir la colaboración de entidades nacionales, internacionales y extranjeras cuando se afecten los derechos de los titulares.

En el año 2020 mediante la expedición de la resolución 385 del 12 de marzo del año 2020, el Ministerio de Salud y Protección Social de Colombia, declaró la emergencia sanitaria en a causa del coronavirus COVID – 19, y la SIC bajo sus funciones, se dirige a los operadores de telefonía móvil, indicándoles como debían suministrar información al DNP y a las entidades que requirieran los datos de los usuarios, con la finalidad de tratarlos, atenderlos y prevenir contagios y la propagación del brote.

Por medio de la "Circular Externa 002 de 27 de marzo de 2020", la SIC recomendó no usar huelleros para recolección de información de datos biométricos, esto buscando prevenir contagios por posible contacto, siendo también precursora de políticas de salud públicas y mediante la Circular Externa No. 008 de 2020, la SIC entregó recomendaciones sobre recolección y trato de datos para cumplir con "protocolos de bioseguridad".

En el año 2020, la SIC bajo las funciones otorgadas en el artículo 21 de la Ley 1581 del 2012, profiere cincuenta y una resoluciones, siendo la resolución 74519 de 2020 y 62132 de 2020 tratadas oficiosamente, pues las demás se adelantaron dentro del marco normal de sus funciones y a solicitud de las personas afectadas en sus derechos y en 2021, la SIC expide 87 resoluciones, las cuales en su mayoría fueron adelantadas a petición de parte.

La SIC En relación al marco normativo bajo el cual se maneja y que se ha llevado a cabo desde la Delegatura para la Protección de Datos Personales, se puede concluir que, las personas naturales o jurídicas que han sido sancionadas por presunta vulneración de datos personales, han presentado reposiciones y/o apelaciones dilatando así el proceso llevado a cabo por la SIC, por lo que se espera la efectividad tanto de la normativa que ampara a la entidad como las funciones que la ley otorga a la SIC para efectos sancionatorios.

Una de las características más importantes que tiene en cuenta la SIC para fundamentar sus decisiones cuando existe vulneración del derecho del habeas data, fue enlistar las políticas internas básicas que deben tener en cuenta las empresas para el manejo apropiado de los datos personales, como son:

1) Tener dispuesto a lo indicado por la ley colombiana y lo que esta le ordene y requiera, para poder seguir con sus operaciones en la nación.

2) La Ley 1581 de 2012, es aplicable a las empresas requeridas pues esta obtiene datos personales de los usuarios por medio de cookies que son aceptadas para el funcionamiento de la plataforma y quedan instalados en los servidores y equipos de las personas que habitan en Colombia y desde allí usan la plataforma.

3) Para aceptar el tratamiento de datos personales por parte de un tercero, se requieren garantías de seguridad de la información, así que, una vez obtenidos estos datos, estos deben pasar por varias etapas de cuidado que evitan situaciones perjudiciales que podrían poner en riesgo inclusive, derechos fundamentales de las personas, por un indebido cuidado en esta información, afectando no solo a los titulares del dato, sino también a los que lo recolectan y los tercerizados.

4) Mejorar e incrementar la capacidad de atender contingencias de seguridad, desarrollar y poner en marcha un sistema de seguridad que otorgara garantías en cuanto a la confidencialidad de la información y poniendo a disposición de sus trabajadores herramientas para que se acercaran a la ley 1581 y estos tuvieran conocimiento de las prerrogativas y alcances jurídicos de la misma.

Por su parte, cuando existe un riesgo y no se ha concretado un daño, la SIC puede tomar medidas preventivas por medio de los requerimientos establecidos en sus resoluciones entre las más relevantes se encuentran:

1) informar a la SIC el número de cuentas correspondientes a nacionales o residentes colombianos, precisando y separando cuales de estas correspondían a menores de 18 años.

2) informar si la empresa recolectaba para ese momento información de menores de edad y de ser el caso, cuál era el paso para seguir para manejar esta información y si contaba con la aceptación y autorización de los padres o tutores de estos menores, para poder tener cuentas en dichas plataformas.

En conclusión, las leyes sobre tratamiento de datos deben ser aplicadas conforme los procesos que se usen para obtener los datos de los usuarios. La legislación colombiana no impide el uso de tecnologías para el manejo de los datos, pero si exige como contraprestación que el trato de estos sea minucioso y acorde a la ley.

Es necesario que quienes crean y manejan tecnologías innovadoras, destinadas a la seguridad de los usuarios, cumplan con lo dispuesto en la ley. La Superintendencia recalca la importancia que adquiere el respeto por la ley, de parte de quienes figuran como encargados de la administración de datos personales, sea cual sea la naturaleza de estos, lo que deja ver la convicción de la SIC como entidad, en su deber de salvaguardar los derechos de los usuarios, realizando funciones de control y vigilancia sobre los datos personales y el manejo que se le da a estos.

Lista de Referencias

Barrera-Campos, J. M. (2020). Regulación sobre protección de datos personales en el mundo digital en el Estado Colombiano. Encontrado en: https://repository.ucatolica.edu.co/handle/10983/25106

Benavides, D., Criollo, L., Garzón, J., Obando, D., Torres, A., Urbano, B., & Riascos, L. (2019). Actos administrativos del director de la Superintendencia de Industria y Comercio de Colombia SIC. Encontrado en: chrome-

extension://efaidnbmnnnibpcajpcglclefindmkaj/http://derechopublico.udenar.edu.co/Invest_%20AA_SIC_2020_4B.pdf

Castrillón Grondona, L. J., & Uribe Posada, M. P. (2017). Vulneración del habeas data y mecanismos de protección en Colombia. Encontrado en: https://repository.upb.edu.co/handle/20.500.11912/3460

Cifuentes Muñoz, E. (1997). El hábeas data en Colombia. *Derecho PUCP*, *51*, 115. Encontrado en: https://heinonline.org/HOL/LandingPage?handle=hein.journals/derecho51&div=9&id=&page=

Circular Externa 002 de 2020 "No uso de "huelleros físicos o electrónicos" de uso masivo para recolectar información biométrica (datos sensibles) con miras a prevenir el contagio del COVID-19 a través de contacto indirecto". SIC, Bogotá, 24 de marzo de 2020. Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/032020/CIRCULAR%20002%20 DE%202020_NO%20USO%20DE%20HUELLEROS.pdf.

Corredor, F. A., Suárez, J. C., & Patarroyo, L. J. (2020). Protección De Datos Personales en Sistemas De Monitorización y Vigilancia Masiva De Personas Ante La Pandemia De Covid-19. Encontrado en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cici.unillanos.edu.co/media2020/memorias/CICI_2020_paper_129.pdf

Cote Peña, L. F. (2016). Hábeas Data en Colombia, un Trasplante Normativo para la Protección de la Dignidad y su Correlación con la NTC/ISO/IEC 27001. Encontrado en: https://repository.usta.edu.co/handle/11634/965

Cuartas Rodríguez, E., & Jaller Escudero, J. D. (2014). *El Habeas Data como Derecho fundamental y la Ley 1581 de 2012 y su decreto 1377 de 2013* (Bachelor's thesis, Universidad EAFIT). Encontrado en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repository.eafit.edu.co/bitstre

am/handle/10784/5376/EL%20HABEAS%20DATA%20COMO%20DERECHO%20FUNDAMENTAL%20Y%20LA%20LEY%201581%20DE%202012%20Y%20SU%20DECRETO%201377%20DE%202013.pdf?sequence=2

Estrada, E. C. M. (2014). Procedencia del habeas data, el derecho a la intimidad y la figura de la prescripción. Las personas erróneamente reportadas en las centrales de riesgo. *Erg@ omnes*, *6*(1), 80-88. Encontrado en: https://revistas.curn.edu.co/index.php/ergaomnes/article/view/456

Galvis Cano, L. (2018). El Panóptico digital de la protección de datos personales en Colombia. Revista Temas. III (12), 125-140. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6749433

Galvis Cano, Lucero (2012). Protección de datos en Colombia, avances y retos. Lebret, (4), 195-213. Disponible en: https://doi.org/10.15332/rl.v4i4.336

Gómez, V. M. (2015). El derecho al olvido: análisis comparativo de las fuentes internacionales con la regulación colombiana. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, (14), 3. Encontrado en: https://dialnet.unirioja.es/servlet/articulo?codigo=7496887

Gómez-Córdoba, A., Arévalo-Leal, S., Bernal-Camargo, D., & Rosero de los Ríos, D. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. *Revista de bioética y derecho*, (50), 271-294. Encontrado en: https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872020000300017

González Segrera, P. (2018). *El rol de la superintendencia de industria y comercio en la protección de los consumidores como autoridad jurisdiccional: un análisis a su eficacia y efectividad material* (Master's thesis, Universidad del Norte). Encontrado en: https://repository.ucatolica.edu.co/handle/10983/2604

Hernández, M., Tamayo, R (2006). El Habeas Data como mecanismo de protección de derechos relacionados con la autodeterminación informativa ante el tratamiento automatizado de datos personales. San Salvador, El Salvador. Universidad de El Salvador.

Maqueo, Moreno & Recio. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. Revista de derecho (Valdivia), 30(1), 77-96. Disponible en: https://dx.doi.org/10.4067/S0718-09502017000100004

Organización de las Naciones Unidas, (2018). Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Disponible en: https://www.ohchr.org/SP/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

Peña, K. I. C., & Montenegr Jaramillo, Y. A. (2022). Protección de Datos Personales en el Marco de la COVID-19: el Caso de CoronApp en Colombia. *Revista de Direito, Estado e Telecomunicações*, *14*(1). Encontrado en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.researchgate.net/profile/Karen-Cabrera-Pena/publication/361265804_Proteccion_de_Datos_Personales_en_el_Marco_de_la_COVID-19_el_Caso_de_CoronApp_en_Colombia/links/62b0e3d389e4f1160c8d2840/Proteccion-de-Datos-Personales-en-el-Marco-de-la-COVID-19-el-Caso-de-CoronApp-en-Colombia.pdf

Pérez-Fernández, O. E. (2017). El habeas data en Colombia: su desarrollo y conexidad con los derechos fundamentales. Encontrado en: https://repository.ucatolica.edu.co/handle/10983/14745

Rojas-Bejarano, M. (2014). Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales. *Novum Jus: Revista Especializada*

en Sociología Jurídica y Política; Vol. 8, no. 1 (ene.-jun. 2014); p. 107-139. Encontrado en: https://repository.ucatolica.edu.co/handle/10983/16577

SIC. (2020). Aspectos prácticos sobre el Derecho de Habeas Data. Disponible en: https://www.sic.gov.co/centro-de-publicaciones?field_global_topic_tid=7037&field_anos_p_value=All

SIC. (2020). Circular 001 del 24 de marzo de 2020. Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/032020/Circular%20001.pdf.pdf

SIC. (2020). Circular Única del 2 de junio de 2022. Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/062022/T%C3%ADtulo%20V%20Proteccion%20Datos%20Res%2028170%20del%2011%20de%20mayo%20de%202022%20%281%29.pdf

SIC. (2020). Circular Única del 29 de mayo de 2020. Disponible en: https://www.sic.gov.co/sites/default/files/normatividad/052020/Ti%CC%81tulo%20V%20Proteccion%20Datos%20Circular%2003%20del%2030%20de%20marzo%202020%29.pdf

SIC. (2020). Guía de datos personales para fines de comercio electrónico. Disponible en: https://www.sic.gov.co/centro-de-publicaciones?field_global_topic_tid=7037&field_anos_p_value=All

SIC. (2020). Guía para el "tratamiento de datos personales" mediante el servicio de computación en la nube. Disponible en: https://www.sic.gov.co/centro-de-publicaciones?field_global_topic_tid=7037&field_anos_p_value=All

SIC. (2020). Guía para la gestión de incidentes de seguridad en el "tratamiento de datos personales". Disponible en: https://www.sic.gov.co/centro-de-publicaciones?field_global_topic_tid=7037&field_anos_p_value=All

SIC. (2020). Políticas para el "tratamiento de datos personales". Disponible en: https://www.sic.gov.co/sites/default/files/documentos/072020/Pol%C3%ADtica%20de%20Tratamiento%20de%20Datos%20Personales%20-%20SIC.pdf

SIC. (2020). Resolución 12169 de 2020. Disponible en: https://www.sic.gov.co/sites/default/files/files/Noticias/2019/Res-1321-de-2019.pdf

SIC. (2020). Resolución 1321 de 2019. Disponible en: https://www.sic.gov.co/sites/default/files/files/Noticias/2019/Res-1321-de-2019.pdf

SIC. (2020). Resolución 68369 de 2020. Disponible en: https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/actos_administrativos/RE68369-2020%20(1).pdf

Trujillo, L. V. P. (2021). Estructuración de los elementos de la responsabilidad del Estado por el uso indebido de los datos relacionados con el estado de salud. Análisis dogmático y biojurídico. *Revista Vía Iuris*, (31), 1-36. Encontrado en: https://revistas.libertadores.edu.co/index.php/ViaIuris/article/view/1126

Vera Vera, O. F. (2020). Confidencialidad de la información y su reglamentación en Colombia. Habeas data. Encontrado en: http://repository.unipiloto.edu.co/handle/20.500.12277/7780