Procedimientos y requisitos que deben cumplir las entidades para salvaguardar los derechos de los titulares de datos personales sensibles en Colombia[1]

Juan Carlos Mesa Álvarez[2]

Carlos Alberto Mena Cuesta[3]

Resumen

Este artículo de revisión documental se realizó con el objetivo de analizar los procedimientos y requisitos que deben cumplir las entidades para salvaguardar los derechos de los titulares de datos personales sensibles en caso de transferencia en Colombia. Para el desarrollo de este estudio se utilizó una metodología cualitativa, a partir de la cual se revisaron, interpretaron y analizaron alrededor de 54 referencias bibliográficas. A partir de los resultados se concluye que, en el país, si bien existe una normativa que permita indicar los lineamientos para el tratamiento de datos, falta eficacia y debido control para el cumplimiento de la misma, además, no hay claridad respecto a las excepciones, los mecanismos de control, las sanciones concretas en caso de fallas en el tratamiento de datos sensibles, acciones como indemnización, entre otros aspectos. Por lo anterior, las empresas colombianas, además de cumplir con los elementos trazados en la Ley 1581 de 2012 y el Decreto Único Reglamentario 1074 de 2015, deben realizar periódicamente una evaluación de impacto frente al tratamiento de datos sensibles, designar un colaborador que se encargue específicamente de la protección de datos sensibles, notificar de manera oportuna en caso de que se vulnere la seguridad de estos datos, entre otras para garantizar el debido tratamiento de datos y, por ende, los derechos de sus titulares.

Palabras clave: datos sensibles; derechos de los titulares de datos; deberes de los tenedores de datos; tratamiento de datos sensibles.

[1] Articulo de revisión para optar a título de Abogados de la Universidad Católica Luis Amigó. Asesor temático:

[2] Estudiante de derecho de la Universidad Católica Luis Amigó. Correo:

[3] Estudiante de derecho de la Universidad Católica Luis Amigó. Correo:

Abstract

This review article was carried out with the objective of analyzing the procedures and requirements that entities must comply with to safeguard the rights of owners of sensitive personal data in the event of transfer in Colombia. To develop this study, a qualitative methodology was used, from which around 54 bibliographic references were reviewed, interpreted and analyzed. Based on the results, it is concluded that, in the country, although there is a regulation that allows indicating the guidelines for data processing, there is a lack of effectiveness and due control for compliance with it, in addition, there is no clarity regarding the exceptions. . . , control mechanisms, specific sanctions in case of failures in the processing of sensitive data, actions such as compensation, among other aspects. Due to the above, Colombian companies, in addition to complying with the elements indicated in Law 1581 of 2012 and the Single Regulatory Decree 1074 of 2015, must periodically carry out an impact evaluation regarding the processing of sensitive data, designate a collaborator who is to place an order specifically, the protection of sensitive data, timely notification in the event that the security of this data is violated, among others to guarantee the adequate processing of the data and, therefore, the rights of its owners.

Keywords: sensitive data; rights of interested parties; duties of data subjects; processing of sensitive data.

Introducción

Cuando se habla de datos personales se hace referencia a toda la información personal que puede incluir número de identificación, fecha de nacimiento, lugar de nacimiento, estado civil, trayectoria académica y laboral o profesional, entre otros elementos. Estos datos, en la actualidad son recolectados y almacenados por entidades públicas y privadas con la finalidad de hacer una individualización de los ciudadanos, clientes o usuarios según sea el caso. Ahora bien, como lo menciona Mendoza (2018), las organizaciones tienen la obligación de mantener la confidencialidad de los datos personales y de solicitar el consentimiento de los titulares cuando

desean enviar o transferir estos datos, dicho de otro modo, las entidades deben velar por dar un tratamiento y salvaguarda rigurosa a la información más aún cuando integran datos sensibles como es el caso del estado de la salud de la persona, sus características físicas, ideología política, vida sexual, orientación sexual entre otros tipos de información que, de ser mal empelada puede generar afectaciones sobre bienes jurídicos de los titulares de la misma.

Meraz (2018), indica que en la actualidad muchas entidades no dan cumplimiento a la regulación en materia de protección de datos personales sensibles, es decir, desatienden el marco jurídico nacional que impone deberes y obligaciones en el tratamiento de datos personales que para el caso de Colombia se da a partir de la Ley 1581 de 2012, la cual busca proteger el derecho que tienes todos los colombianos a conocer, actualizar y ratificar la información dispuesta en bases de datos o archivos que sean susceptibles de tratamiento por parte de entidades públicas o privadas en Colombia. Este incumplimiento es visibilizado por la Superintendencia de Industria y Comercio (2022), quien indica que alrededor de 24.424 organizaciones públicas y privadas que funcionan en Colombia no han puesto en marcha todavía ninguna política de protección de dato personales.

Desde una perspectiva jurídica, el procesamiento, uso y almacenamiento de información requiere seguridad, a partir de la cual los titulares pueden confiar en el tratamiento de esta información, y los tenedores de la información pueden garantizar el buen uso y protección de estos datos (Meraz, 2018). De allí que, cuando no existan políticas de protección de datos personales o estas no se cumplan se puedan generar afectaciones en los titulares, quienes están revestidos de facultades para demandar las garantías que le correspondan.

El problema se agrava cuando se desconocen procedimientos y requisitos que las entidades deben cumplir para la transferencia de datos personales. Lo anterior, genera que entidades a las cuales se les confiere esta información personal con estrecha autorización del usuario no tengan un tratamiento riguroso sobre cada uno de los datos recolectados lo que puede llegar a romper la cadena de custodia que requieren los mismos lo que da paso a que se filtren los datos personales sensibles en otras entidades y, por tanto, se transgredan derechos como es el

caso del derecho a la intimidad, derecho a la seguridad, derecho a la privacidad y derechos conexos.

Con base a lo anterior, el presente estudio busca responder al siguiente problema jurídico: ¿Qué procedimientos y requisitos que deben cumplir las entidades para salvaguardar los derechos de los titulares de datos personales sensibles en caso de transferencia en Colombia? Por tanto, se plantea como objetivo general: Analizar los procedimientos y requisitos que deben cumplir las entidades para salvaguardar los derechos de los titulares de datos personales sensibles en caso de transferencia en Colombia.

Para alcanzar la pretensión del estudio se plantean los siguientes objetivos específicos: el primero de ellos, es describir las generalidades normativas relativas a la protección de datos personales en Colombia. El segundo, identificar la manera en la cual el tratamiento inadecuado de datos personales sensibles por parte de las empresas puede vulnerar los bienes jurídicos de los ciudadanos colombianos. Finalmente, establecer las prácticas internacionales recomendadas en materia el tratamiento de datos que pueden ser adoptadas por Colombia.

Este artículo de revisión es pertinente, en la medida que otorga al lector claridad frente a los procedimientos y requisitos que deben cumplir las entidades para salvaguardar los derechos de los titulares de datos personales sensibles en Colombia. En esta misma línea, se indica que la presente revisión permitirá vislumbrar la manera en la cual el desconocimiento de estos procedimientos puede vulnerar los derechos que tiene los titulares y tenedores de la información, especialmente, del derecho a la intimidad y conexos; con la intención de que se avizore la yuxtaposición en que se encuentra dicho derecho fundamental con la práctica de los enunciados procedimientos.

Metodología

Este estudio se desarrolla a partir del modelo de investigación de la Dogmático-Jurídico, el cual en palabras de Tantaleán (2016), se centra en el abordaje de un problema jurídico a partir

del análisis de la norma jurídica. Dicho de otro modo, este modelo de investigación permite interpretar un fenómeno a partir de las fuentes formales del derecho objetivo. En consonancia con lo anterior, Valencia y Marín (2018), señalan que el modelo dogmático de investigación es explicado desde la hermenéutica, situando a esta última como una estrategia que permite la comprensión de lo textual, con el animo de hallar un significado lógico. En este caso lo que se busca es hacer una interpretación del objeto de estudio sin hacer ninguna inferencia o alteración sobre las variables que lo componen, por el contrario, describiéndolo desde el ordenamiento normativo jurídico vigente.

De igual modo, se indica que esta es una investigación con un enfoque cualitativo-documental el cual, en palabras de Nizama y Nizama (2020) está orientado a la interpretación y comprensión de caso concreto de derecho, a partir de la deconstrucción, análisis y reintegración de elementos teóricos que han sido desarrollados por otros autores de manera precedente. En línea con lo anterior, Botero (2003), manifiesta que el tipo de enfoque cualitativo-documental posibilita construir conocimiento partir del análisis y comprensión de los documentos, en este caso documentos referidos a los procedimientos y requisitos que deben cumplir las entidades para salvaguardar los derechos de los titulares de datos personales sensibles en Colombia.

El método de investigación de este estudio corresponde al descriptivo, el cual de acuerdo con Rivera (2007) permite descomponer un tema jurídico para, posteriormente dar a conocer las características que lo integran, interpretarlas y llegar a conclusiones. Al respecto, Villabella (2015), indica que el método descriptivo no se basa simplemente en la descripción de hechos sino una búsqueda intencional para explicar o interpretar un fenómeno jurídico.

Finalmente, se hará uso de la técnica de análisis documental, que en palabras de Dulzaides y Molina (2004) es una técnica que permite la interpretación de documentos de forma sistemática y unificada. Por su parte Peña y Pirela (2007), señalan que la técnica de análisis documental permite a los investigadores procesar de forma analítica y sintética los documentos. En este punto se indica que el instrumento a emplear será una matriz documental, ello con la pretensión de

organizar la información recolectada y contrastarla para de este modo encontrar patrones (convergencias y divergencias) entre ellos, y dar respuesta a cada uno de los objetivos planteados.

Desarrollo

1. Generalidades normativas relativas a la protección de datos personales en Colombia

Leyes y decretos relevantes

Una de las leyes clave respecto a la protección de datos personales en Colombia, es la Ley Orgánica 1266 de 2008, la cual indica elementos sobre el Habeas Data y el manejo de la información que se encuentra contenida en bases de datos personales. Esta Ley protege el derecho constitucional que tiene todo ciudadano colombiano a conocer, actualizar y rectificar la información recogida en las bases de datos, además de la libertad y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales (Monsalve, 2017; Pérez, 2016; Cuartas y Jaller, 2014).

Sin embargo, la principal legislación relacionada con la protección de datos en Colombia es la Ley 1581 de 2012 por la cual se establecen las disposiciones dirigidas a la protección de datos personales. Esta ley fue promulgada para garantizar el derecho constitucional de las personas a conocer, actualizar y rectificar la información que sobre ellas se ha recopilado en las bases de datos, y para asegurar que sus datos personales sean tratados de acuerdo con su derecho a la privacidad.

Como señala Guzmán (2016) la Ley de Protección de Datos Personales aplica a toda persona física y/o jurídica pública o privada que realice cualquier tipo de actividad que involucre el tratamiento de datos personales, ya sea que los datos sean recolectados en Colombia o en el extranjero. El incumplimiento de la Ley de Protección de Datos Personales puede resultar en multas, sanciones y otras sanciones (Bautista-Avellaneda, 2015). Por tanto, es de gran

importancia que las organizaciones que procesan datos personales en Colombia se aseguren de cumplir con la ley y contar con las medidas adecuadas para proteger los datos personales.

En palabras de Arboleda (2014), la Ley 1581 de 2012 se desarrolla a partir del derecho fundamental a la intimidad, el cual está protegido por la Constitución Política de Colombia, particularmente en su artículo 15 "todas las personas tienen derecho a la intimidad personal y familiar, la protección de su buen nombre, así como conocer, actualizar y rectificar la información que haya sido recogida en bases de datos públicas y privadas". Bajo esta perspectiva, la protección está asociada a la noción de libertad individual, buen nombre, honor e inviolabilidad de la correspondencia.

En consonancia con lo anterior, Alonso y Rodríguez (2017), señalan que el ordenamiento jurídico colombiano reconoce el derecho a la intimidad como un derecho humano fundamental, el cual está protegido por el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos de 1969, de los cuales Colombia es parte. Este derecho, según González (2017), incluye el derecho a controlar el acceso a la información y al espacio personal de uno, el derecho a participar en actividades sexuales consensuales sin interferencias y el derecho a formar relaciones íntimas con otros sin temor a discriminación o persecución. Sin embargo, es importante señalar tal como lo plantea Covarrubias (2015), que el ejercicio de este derecho también debe equilibrarse con el interés público y la protección de otros derechos fundamentales, como el derecho a la vida, la salud y la seguridad pública.

Al continuar con la revisión, la Ley de Protección de Datos también se ha desarrollado en las siguientes normas: el Decreto 1377 de 2013 que Reglamenta Parcialmente la Ley de Protección de Datos Personales; el Decreto 1081 de 2015 que regula la Presidencia de Colombia e incluye disposiciones de ley de protección de datos; y el Decreto 255 de 2022 que regula las leyes corporativas vinculantes con el fin de certificar buenas prácticas en materia de protección de datos y su transferencia a terceros países. También es menester resaltar que existen otras leyes y regulaciones que se aplican a industrias o tipos de datos específicos, como la Ley 1439 de 2011

relativa a la Protección de Información de Salud y el Decreto 2555 de 2010 que se centra en la Protección de Información Financiera.

En este punto, es importante indicar que en Colombia los datos pueden clasificarse en: datos privados, datos semiprivados, datos públicos y datos sensibles. En el caso del presente estudio se hace énfasis en los datos sensibles, conceptualizados como aquellos datos que afectan la intimidad del titular y cuyo uso ineducado puede generarle exclusión de tipo racial, orientación de género, preferencia política, etc.

Respecto al marco normativo sobre datos personales sensibles en Colombia, es importante indicar que la Ley más relevante es la 1581 de 2012, la cual, particularmente en su título III "Categorías especiales de datos", y en los artículos 5 y 6, define a los datos sensibles e indica su tratamiento, respectivamente. La Corte Constitucional también se ha pronunciado en diversos momentos respecto a los datos sensibles. Por ejemplo, en la Sentencia C-748 de 201131 , se expuso que los datos sensibles hacen parte del núcleo esencial del derecho a la intimidad. De igual forma, en la Sentencia T-114/18 se aborda el acceso a los datos sensibles recopilados por los circuitos cerrados de televisión. Otros de los pronunciamientos son las Sentencias SU139 de 21 y T-450 de 22 que abarcan el derecho fundamental al habeas data y datos sobre antecedentes penales y requerimientos judiciales., en ambas se retoma el concepto de dato sensible y como debe ser su tratamiento.

Pautas y ámbitos de aplicación normativa datos personales

Al efectuar una revisión la literatura, se identifica que la principal autoridad de protección de datos en Colombia es la Superintendencia de Industria y Comercio (SIC), la cual ha elaborado una lista exhaustiva de lineamientos con el fin de brindar claridad a las organizaciones en la implementación de la Ley de Protección de Datos.

De acuerdo con Vásquez (2021), respecto al ámbito de aplicación de la normativa referida a datos este puede ser personal, territorial y material. Respecto al alcance personal, el artículo 2

de la Ley de Protección de Datos Personales establece el ámbito de aplicación al señalar que los principios y disposiciones contenidos en la ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de carácter público o privado.

Por lo anterior, cualquier dato personal que sea transferido y registrado en una base de datos estará sujeto a la Ley de Protección de Datos Personales. Así, pues como lo indica Caballero (2015), aplica a todas las personas naturales y jurídicas que recopilen, procesen, almacenen o transfieran datos personales en el país, independientemente de su nacionalidad o personalidad jurídica. Es menester resaltar que la ley cubre tanto el sector público como el privado y se aplica a todo tipo de datos personales, incluidos datos confidenciales relacionados con la raza, etnia, opiniones políticas, creencias religiosas, orientación sexual, estado de salud y antecedentes penales de un individuo.

Frente al ámbito territorial el artículo 2 de la Ley de Protección de Datos Personales afirma que se aplicará a los datos personales tratados en territorio colombiano; o cuando el responsable o encargado del tratamiento no esté establecido en territorio colombiano pero su ley sea aplicable en virtud de normas y tratados internacionales.

Finalmente, frente al ámbito material la ley establece que la recopilación y el procesamiento de datos personales por cualquier medio, incluidos los registros electrónicos y físicos requiere el consentimiento del interesado, establece obligaciones para los responsables del tratamiento y exige transparencia y responsabilidad en el procesamiento de datos personales. Cabe resaltar que, el artículo 19 de la Ley de Protección de Datos Personales establece a la SIC, específicamente a su Delegación de Protección de Datos Personales (DPDP), como la autoridad encargada de hacer cumplir las leyes de protección de datos en Colombia.

Según la SIC (2023) la DPDP supervisa el cumplimiento de las leyes de protección de datos de Colombia, incluida la Ley de Protección de Datos Personales y sus regulaciones relacionadas, además, tiene la facultad de investigar y sancionar a personas y organizaciones que

violen las leyes de protección de datos e imponer multas y otras sanciones. Ñustes, Pabón Y Romero (2021), indican que la DPDP también brinda orientación y apoyo a personas y organizaciones sobre cómo cumplir con las leyes de protección de datos, y es responsable de mantener el Registro Nacional de Bases de Datos (RNBD), que es una lista de todas las bases de datos que contienen datos personales en Colombia.

Elementos legales clave para comprender el alcance de la protección de datos personales

Es importante mencionar algunos elementos legales clave para entender a cabalidad la manera en la cual se gestiona la protección de datos personales, entre los elementos más relevantes se encuentran: acción de consentir; contrato con el interesado; obligaciones legales; intereses del interesado; interés público; intereses legítimos del responsable del tratamiento; y, bases jurídicas en otras instancias. Los cuales se conceptualizarán, a continuación.

Frente a la acción de consentir, el artículo 5 de la Ley de Protección de Datos Personales indica que los responsables del tratamiento deberán establecer procedimientos para solicitar, a más tardar en el momento de la recogida de los datos, la autorización del interesado para tratar sus datos y notificarle que los datos serán recogidos personalmente, así como para cualquier finalidad específica que requiera consentir.

De acuerdo con la Asociación Colombiana de empresas de investigación de mercado y opinión pública (2020), en caso de cambios significativos en el contenido de la política de tratamiento de datos respecto de la identidad del responsable del tratamiento y de las finalidades del tratamiento que puedan afectar a la autorización, el responsable del tratamiento deberá comunicar dichos cambios a los interesados a más tardar en el momento de la implementación y debe obtener nuevos permisos de personas relevantes.

Respecto a la autorización para el tratamiento de datos personales, el artículo 25 del Decreto 1377, estipula que el contrato celebrado entre el responsable y el interesado para el tratamiento de datos personales deberá especificar el alcance del tratamiento, las actividades que

el encargado llevará a cabo por cuenta del responsable y las obligaciones del encargado del tratamiento.

Al ahondar en las obligaciones legales, según el artículo 10 de la Ley de Protección de Datos Personales, no es necesario el consentimiento del interesado cuando la información sea requerida por una entidad pública o administrativa en el ejercicio de sus funciones legales o por orden judicial. En esta misma línea, el interés del interesado y el interés público son descritos en el artículo 10 de la citada Ley, donde se establece que no es necesario el consentimiento del interesado en casos de urgencia médica o sanitaria.

Respecto a los Intereses legítimos del responsable del tratamiento, la norma indica que el tratamiento de los datos requiere el consentimiento previo e informado del interesado, que deberá obtenerse por cualquier medio previa consulta. No obstante, si existe una excepción clara a este principio general, se permitirá el tratamiento de datos por parte del responsable y/o responsable del tratamiento.

Finalmente, al ahondar en las bases jurídicas en otras instancias, según el artículo 10 de la Ley de Protección de Datos Personales no es necesario el consentimiento del interesado en casos de datos de carácter público; procesamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; y datos relacionados con el Registro Civil.

Obligaciones del responsable del tratamiento de los datos sensibles

Es importante indicar que, de acuerdo con la normativa vigente no existe obligación de notificar las actividades de tratamiento de datos, sin embargo, en el caso de la transferencia de datos, esta si tiene limitantes; por ejemplo, la transferencia internacional de datos personales está prohibida a países que no puedan proporcionar niveles adecuados de protección de datos, salvo excepciones indicadas por el articulo 6 de la Ley 1581 de 2012. En este caso, se recomienda que los responsables del tratamiento de datos desarrollen procesos que les permita garantizar su uso adecuado, más aún cunado estos son sensibles; dentro de esas acciones se resalta: generar una descripción a detalle del procesamiento de datos; evaluar los riesgos inherentes a los derechos y

libertades de los titulares de los datos; clasificar lo riesgos y establecer las medidas para mitigarlos.

Los responsables de los datos que estén sujetos a registrar sus bases de datos ante el Registro Nacional de Bases de Datos – RNBD, están en la obligación de cumplir los plazos de presentación de esta información, en consonancia con el Decreto 090 del 18 de enero de 2018. De igual forma, los responsables de los datos deben garantizar la información mínima que debe contener el RNBD y los términos y condiciones bajo los cuales bases de datos sujetas a la aplicación de la Ley de Protección de Datos Personales deben cumplir (Decreto 866 de 2014 y Decreto 1074 de 2015).

Es importante indicar que los responsables del tratamiento de los datos sensibles no están obligados por ley a evaluar el impacto de la protección de datos o hacer trazabilidad de los mismos, sin embargo, como lo establece Balcázar (2020), se recomienda que estos responsables sigan algunos estándares de protección de datos para, de este modo, tener mayor control sobre los riesgos derivados del tratamiento de esta información.

2. Vulneración de bienes jurídicos de los ciudadanos colombianos a partir del inadecuado uso de los datos sensibles

La protección y el tratamiento efectivo de datos sensibles en Colombia presenta diversos desafíos, en la medida que, pese a que existen disposiciones constitucionales y normativas frente al tema, en la actualidad se carecen de los mecanismos de seguimiento y control que garanticen en un cien por ciento que los tenedores de los datos salvaguarden la confidencialidad y con ello, los derechos de los titulares de dichos datos. Lo anterior, en palabras de Sánchez (2021), puede generar afectaciones inconmensurables a los titulares en materia de derecho a la intimidad, derecho a la privacidad, derecho a la identidad y conexos, lo que, a su vez, puede tener efectos negativos a nivel personal, familiar, laboral y social.

Newman (2015), manifiesta que para identificar el nivel de afectación que se desprende del tratamiento inadecuado de datos sensibles, es importante revisar la cercanía de esta acción con relación al núcleo del derecho fundamental que pueda ser vulnerado. Por tanto, la esfera más íntima, que generalmente es donde se desarrollan los datos sensibles, debe tener mayores garantías y mecanismos de protección; mientras que, en la esfera privada o en el ámbito personal, la información es más flexible y, en algunos casos, puede ser compartida con otras personas, por tanto, su protección es menor.

A continuación, se hace un análisis de cómo pueden ser afectados los derechos de los titulares de datos sensibles, si estos últimos no tienen un correcto tratamiento. Cabe resaltar en el siguiente apartado se profundiza en datos sensibles relativos al origen racial, opiniones políticas, convicciones religiosas, afiliación sindical, y aquellos relacionados con la salud, pero para efectos del presente artículo de revisión no se profundiza en otros tipos de datos sensibles indicados en el articulo 5 de la Ley 1581 de 2012, entre ellos los datos que develen la pertenencia a organizaciones sociales, datos relativos a la vida sexual y datos biométricos.

Tratamiento de datos sensibles que revelen origen racial, opiniones políticas y convicciones religiosas

La discriminación étnico-racial se expresa cuando una persona asocia que un individuo afrodescendiente o indígena tiene rasgos intelectuales inferiores, características culturales que no se articulan al estatus quo y una personalidad concreta que se alinea precisamente a su color de piel u origen étnico (Viveros, 2007; Chirix y Sajbin, 2019). En Colombia la discriminación por motivos raciales y étnicos persiste, esto es afirmado por autores como Murillo (2022) quien, además, plantea que las personas que integran grupos diferenciales étnico-raciales se encuentran en un escenario complejo pues, generalmente, son percibidas con base a prejuicios que las deja en una situación desventajosa frente a las personas con características fenotípicas o genotípicas generalmente aceptadas (blancos y mestizos).

Por lo anterior, es que algunas personas deciden que los datos referentes a su origen étnico-racial sea confidencial, ya que, develar información de este tipo en determinados espacios académicos, laborales, comunitarios, políticos, puede generar un prejuicio que lleve a que algunas personas los encasille, clasifique, minimice e incluso cosifique (Fallada, 2012), solo por el hecho de ser "diferentes". En palabras de Ordóñez (2019), cuando se revelan datos sensibles sin autorización de los titulares no solo se está vulnerando el derecho que estos tienes a su intimidad y privacidad, sino que, como lo plantea Newman (2015) conlleva el riesgo de aumentar la discriminación.

Respecto a los datos sensibles referidos a las opiniones políticas, López, Farriols y Hormazábal (2019), señalan que estos deben ser salvaguardados para garantizar el honor, la intimidad personal y el pleno ejercicio de los ciudadanos a ejercer su voto y tener una inclinación política sin perjuicio de ser discriminado. Como lo indica García (2019), cuando se recopilar datos sensibles frente a las opiniones políticas y estos no tiene un correcto tratamiento se arrebata el poder y el control a los titulares sobre dichos datos, acción que es una afrenta contra la libertad ideológica y es especialmente grave ya que, por ejemplo, los partidos políticos para lograr su posicionamiento o el desprestigio a la oposición, pueden utilizar estos datos sensibles como estrategia de manipulación y total ausencia de transparencia.

En Colombia, la Superintendencia de Industria y Comercio- SIC (2022), indicó que, particularmente, en tiempo de campañas los movimientos políticos, partidos políticos y candidatos deben asegurar el manejo de datos sensibles, para lo cual deben tener en cuenta las disposiciones de la Ley 1581 de 2012 (artículos 4, 9, 12, 17, 18), y el Decreto 13774 de 2013 (artículo 4), que, en síntesis indica que estos agentes políticos no pueden emplear medios fraudulentos para recolectar y hacer el tratamiento de los datos; deben hacer uso exclusivo de estos datos sensibles para fines específicos y debidamente informados a los titulares; deben asegurar las medidas administrativas, técnicas y humanas para brindar seguridad a los datos sensibles; además, que ninguna actividad política puede condicionarse al hecho de que la persona suministre o no sus datos sensibles.

Frente a las convicciones religiosas, Hernández (2004), manifiesta que, cuando estos datos sensibles no son salvaguardados, el titular de los mismos puede enfrentarse discriminación al momento de postularse a un puesto de trabajo, incluso, como explica Pelayo (2019) puede ser sometido a prejuicios en donde se le considere un delincuente o una persona que puede atentar contra la integridad de los demás como sucede, por ejemplo, cuando el titular de los datos profesa la religión del Islam. De acuerdo con Cano (2010), algunos de los problemas que pueden generarse es cuando una persona bautizada en la iglesia católica decide cambiar de religión o no hacer parte de ninguna y las comunidades eclesiásticas no cancelan los datos obrantes en los asientos de los libros de bautismo, aun cuando estos últimos revelan las creencias religiosas de la persona, esta situación se agrava, según Rodríguez (2008), cuando no hay un control frente a quien puede solicitar un certificado de bautizo, pese a que es un dato sensible, como ocurre el algunas iglesias.

Es menester resaltar que el derecho fundamental a la protección de datos sensibles está configurado bajo dos vertientes: una defensiva y una activa. Desde la vertiente defensiva se postula que todos los datos sensibles referidos a la raza, inclinación política y convicción religiosa es íntimo; sin embargo, la vertiente activa, indica que hay una facultad positiva frente al control de estos datos cuando estos sin enfrentados al derecho a la información.

Tratamiento de datos sensibles referidos a afiliación sindical.

Dentro de los datos sensibles que pueden afectar el ámbito laboral de las personas cuando estos no tiene un correcto tratamiento son aquellos referidos a la afiliación sindical. Como lo expresa De Val (2020), cuando no hay un buen manejo de este tipo de datos se puede generar graves impactos sobre las las relaciones de trabajo e incluso, afectaciones que pongan en riesgo la integridad, bienestar y vida del afiliado, máxime en países como Colombia donde, según Gallo (2022), aun persisten los casos de violencia antisindical.

Así pues, los datos de afiliación sindical deben protegerse porque es un derecho personal y exclusivo del trabajador tener libertad de pertenecer a un sindicato, promocionar y defender sus derechos laborales, sin ir en detrimento de su seguridad. Como lo plantea Mercader y Puebla

(2018) tampoco se puede indagar en torno a la vinculación de un trabajador a un sindicato, en la medida que, esto podría generar que dicho trabajador sufra algún tipo de menoscabo en su situación profesional o económica en la empresa a la cual pertenece.

El mal tratamiento de datos de afiliación sindical puede incentivar la discriminación a las personas que hacen parte de estas corporaciones particularmente, en lo que respecta la admisión al empleo y renovación de contratos, esto ocurre, por ejemplo, cuando los datos se filtran en las llamadas "listas negras" que contienen los nombres de los sindicalistas, cuando estas listas negras son conocidas por las empresas, muchas de estas desisten de contratar a quienes están señalados por que no lo consideran conveniente. De igual modo, como lo resaltan Mercader y Puebla (2018), cuando estos datos sensibles son mal usados se puede generar un daño en la reputación y buen nombre del trabajador vinculado al sindicato, lo que, puede causar afectaciones en bienes jurídicos como el derecho al trabajo, derecho al mínimo vital, derecho a la honra y buen nombre, derecho a la privacidad e intimidad, entre otros.

Tratamiento de datos sensibles relativos a la salud

Los datos relativos a la salud física o mental de las personas se introducen en la categoría especial de datos sensibles, en la medida que, según Domínguez (2020), requieren protección adicional ya que pueden llegar al núcleo mismo de un ser humano. Como lo plantean Outomuro y Mirabile (2012), los datos de salud entran en el ámbito más íntimo de la persona, de allí que la divulgación no autorizada de los mismo puede dar lugar a diversas formas de discriminación y violación de los derechos fundamentales. En este punto, es menester resalta que, según Groningen (2020) los datos sensibles merecen una protección específica ya que el contexto de su procesamiento podría crear riesgos importantes para los derechos y libertades fundamentales, entre los cuales se incluyen el derecho a la honra y buen nombre, el derecho a la intimidad, el derecho a la privacidad y afines.

Al respecto, Galvis (2012), plantea que los datos sensibles son un claro indicador de que la intimidad está en juego. Un caso concreto de esta situación se produce cuando el titular de los

datos, por ejemplo, padece una patología como el virus de la inmunodeficiencia humana -VIH y sus datos no se protegen de forma adecuada (Aguirre y Sánchez, 2023), es decir, que el personal que interactúa con sus datos clínicos no es consciente de la importancia del secreto y de la confidencialidad de esta información (Key M y col, 2021), esto da a lugar que sobre paciente recaigan prácticas de exclusión y discriminación (López, 2011).

Peñarete y Oviedo (2020), explican que la protección de datos sensibles en el sector de la salud no siempre se cumple bajo los parámetros establecidos por la ley. Lo anterior, se debe principalmente a que la información sensible, en ocasiones, es manipulada por diversos individuos. Un claro ejemplo de esto., es cuando un tercero hace la solicitud de historia clínica (el empleador al trabajador) o incapacidades (donde se puede visualizar el diagnóstico). De igual modo, esta trasgresión de datos sensibles relacionados con la salud puede darse por personal administrativo de las Instituciones de Salud, como es el caso de personal de archivo y contabilidad.

En este punto, se devela un problema en el cumplimiento de la normatividad respecto al tratamiento de los datos sensibles, ya que no se tiene en cuenta los lineamientos respecto al acceso y la circulación restringida de la información (Caro, 2015). Para evitar tal situación Rojas (2014), establece que en todos los procesos en donde se cuente con información médica sensible debe haber un responsable del tratamiento de la información, pero, así mismo, como lo plantean Arboleda y Anaya (2018), las Instituciones de Salud deben contar con toda la capacidad humana, técnica, administrativa y de infraestructura para garantizar su seguridad, lo anterior, no solo permitirá controlar elementos como la adulteración o pérdida de los datos, sino su acceso fraudulento.

Al revisar el tema de los datos sensibles en Colombia, hay una premisa fundante: salvaguarda de la intimidad al tiempo que se valoren los principios que obliguen al sujeto a inclinarse por la transparencia, así como la finalidad de la difusión de los datos. Como se evidenció a lo largo de este segundo apartado, si bien pueden existir excepciones al tratamiento de datos sensibles, por ejemplo, cuando se trata de fines estadísticos, históricos o científicos, lo

que debe priorizarse es la generación de medidas y mecanismos que permitan la supresión de la identidad de los titulares, de este modo, estos últimos pueden conservar su integridad, intimidad y privacidad.

3. Prácticas en materia de tratamiento de datos sensibles que pueden ser adoptadas por Colombia.

Claro está que el incumplimiento de la Ley de protección de datos expone a las organizaciones a sanciones de tipo económico y operativo, las cuales pueden generar un declive reputaciones de las mismas. De acuerdo con la normativa vigente, las sanciones económicas pueden ascender a 2.000 SMMLV, sin embargo, las sanciones operativas pueden ser más rígidas, ya que van desde la suspensión de actividades relacionadas al tratamiento hasta por seis (6) meses, hasta el cierre temporal o, cierre definitivo de operaciones relacionadas con tratamiento de datos y de datos sensibles. Para dar una clara idea del alcance de las sanciones económicas y operativas, a continuación, se muestran algunos casos reales, en donde se sancionaron algunas empresas en Colombia.

Caso Socialatom Colombia S.A.S

Ante la presunta vulneración de datos personales por parte de la empresa Socialatom Colombia S.A.S, la SIC realizó un proceso de inspección el cual se derivó en una multa de $54.546.380 y ordenes administrativas referidas a los datos y autorizaciones de los titulares (Ortiz, 2019). Según el reporte de la SIC (2019), la empresa no tenía aviso de privacidad, carecía de una política de tratamiento de datos, no tenía manual de procedimientos, además, no informaba a los empleados sobre la finalidad del tratamiento de sus datos, algunos de estos sensibles, en tanto develaban aspectos relativos a su convicción religiosa y estado de salud.

Caso Galvis Arquitectos EU

A partir de una visita de inspección que la SIC (2019) realizó en la empresa Galvis Arquitectos EU tras un incidente de seguridad (Robo de computadores), se identificó que la empresa no tenía medidas de protección de datos personales sensibles, además, que no tenía medidas preventivas ni correctivas para la custodia y tratamiento de las bases de datos con información de sus colaboradores, clientes y proveedores. Otro hallazgo de la SIC, demostró que la empresa no sabía a cuantas personas se había afectado con la pérdida de las bases de datos, además, que la empresa actuó de manera negligente en lo que se refiere a dar respuesta oportuna a los requerimientos de la SIC, de allí que se le impusiera una multa de $ 5.792.812 (Escuela de Privacidad, 2019).

Centro Educativo Superior

Un titular de información en tenencia de la empresa Centro Educativo Superior presentó una queja ante la SIC, indicando que esta institución no contaba con los procedimientos señalados por la ley respecto a la protección de datos sensibles, en tanto, no tenía política de tratamiento de datos, manuales o acciones que garantizaran la confidencialidad. Además de comprobar lo anterior, la SIC identificó que en la institución incumplió con su deber especial del tratamiento de información personal sensible de niños, niñas y adolescente.

Este caso es abordado en la Resolución 5848 de 2019 la SIC, quien particularmente indica que la institución educativa no les informó a los titulares de la información (menores de edad) que no estaban obligados a autorizar el tratamiento de datos y tampoco les informó con antelación cuales de los datos solicitados en la matrícula eran sensibles y la finalidad de su tratamiento, teniendo en cuenta que se solicitó información relativa a tipo de sobre, estado de salud, estrato social, condición de desplazado, entre otros datos. De allí que se le impusiera a la institución una sanción de $1.256.230.

Caso Multilabor Servicios e Insumos

A través de la Resolución 2206 de 2018, la SIC indica que la empresa Multilabor Servicios e Insumos Ltda., cometió una vulneración frente al tratamiento de datos sensibles. La

organización en mención hizo la recolección de información biométrica de sus empleados por medio de registro de huella dactilar sin indicarles a los titulares de los datos que ellos no estaban obligados a autorizar la recolección ni tratamiento de dichos datos, en la medida que entran en la categoría de sensibles de acuerdo a la normativa vigente en Colombia. Respecto a este caso Figueroa y Pérez (2020), indican que la empresa Multilabor Servicios e Insumos vulneró los literales b y c del artículo 17 de la Ley 1581 de 2012, en tanto no solicitaron la copia de la autorización del titular de los datos ni informaron debidamente al titular sobre la recolección de los datos biométricos, además, según los autores, la empresa también vulneró el artículo 2.2.25.2.3 del Decreto Único Reglamentario 1074 de 2015 referido a la autorización para el tratamiento de datos sensibles.

Tratamiento de datos sensibles

En el caso de los datos personales sensibles, las empresas tenedoras de los mismos tiene una responsabilidad reforzada, por ende, deben llevar mayores y mejores controles de seguridad que permitan asegurar el uso legítimo y cierto de los datos y las restricciones de acceso y transferencia. De acuerdo con Arboleda (2018), diversas son las faltas que las empresas pueden cometer a la hora de recolectar datos sensibles: en primer lugar, para algunas organizaciones es difícil la identificación y definición de procesos de la cadena productiva que implican tratamiento de datos sensibles. En segundo lugar, las empresas no desarrollan planes de control que posibiliten verificar si la normativa vigente frente a protección de datos se cumple a cabalidad. En tercer lugar, una falla recurrente es que rara vez las organizaciones hacen seguimiento a las dadas de baja o revocatoria de los titulares de los datos.

Arboleda (2018), identifica algunos errores recurrentes que las empresas tienen al momento de salvaguardar los datos sensibles. Uno de esto errores es negar al titular el ejercicio de su derecho de hábeas data, lo que quiere decir que en algunos casos las empresas dejan de atender las solicitudes de los duelos de los datos frente al ajuste, actualización o supresión de los mismos. Otro de los errores recurrentes, se refiere a que las empresas entreguen datos a terceros para fines como la publicidad sin el consentimiento expreso del titular de los datos. Así mismo,

se reconoce que otro de los errores que comenten las empresas es cuando no poseen las medidas de seguridad necesarias para garantizar que, en caso de hurto de equipos o fallas informáticas los datos sensibles de las personas no queden expuestos.

En atención a lo anterior, Castro (2020) en su estudio indica algunas medidas que internacionalmente se han adoptado para hacer un uso adecuado de estos datos y que pueden ser adoptadas en Colombia para disminuir los casos en donde las empresas vulneran el correcto tratamiento de los saros sensibles.

La primera medida es que las empresas que ostenten la calidad de tenedoras de datos sensibles informen de forma oportuna y clara a los titulares de los datos sobre el derecho que tiene de retirar la autorización del tratamiento de datos. En otras palabras, la empresa debe explicar al cliente que en cualquier momento puede desistir de que sus datos sean usados por la empresa, esta acción le permitirá al titular tener un mayor control sobre su información personal, además, le brindará seguridad. Lo que se busca no es que las empresas solo informen, sino que realicen una acción pedagógica sobre el cliente.

La segunda medida, es que la empresa conserve la copia del consentimiento en donde quede clara la relación de representación del titular y quien actúa en su nombre. Básicamente es un comprobante de que quien actúa en nombre de otro tenga la autorización y esté facultado para hacerlo. Por otro lado, la tercera medida se refiere a la temporalidad y culminación del uso de los datos. Dicho de otra manera, las empresas que sean tenedoras de datos sensibles única y exclusivamente podrán usarlos y conservarlos en el tiempo convenido y autorizado por el titular de los datos. De igual modo, estos datos sensibles no pueden ser usados para fines de la empresa y deben de contar con medidas extra de seguridad por el tipo de dato que son.

Estas medidas de seguridad frente a los datos sensibles pueden funcionar siempre y cuando las empresas no las conciba y las implementen meramente como un acto protocolario, sino que comprendan los riesgos que conlleva el tratamiento de los datos sensibles y la importancia de identificar, clasificar y analizar dichos riesgos para con ello, crear estrategias y

tomar medidas que les permitan asegurar de forma efectiva este tipo de datos. El solo hecho de que los tenedores de la información envíen un correo electrónico con información sensible de los titulares, expone a una filtración de datos; el solo hecho de no informar al titular sobre el uso de los datos, es una vulneración de la normativa vigente en materia. Por lo anterior, las empresas deben adquirir conocimientos, asegurar el cumplimiento de la ley, generar buenas prácticas a seguir para proteger los datos sensibles ya que con ello no solo se salvaguardan los derechos de sus titulares, sino que se evitan sanciones económicas y operativas, las cuales tiene efectos sobre la credibilidad y buen nombre de la organización.

Conclusiones

Tras el desarrollo del presente artículo de revisión, se concluye que si bien Colombia tiene un gran desarrollo en torno al tratamiento de datos personales y se realizan procesos de inspección y control en algunos tenedores o responsables de datos (empresas), es claro que aún no se cuenta con una normativa clara y extensa frente a la garantía de los datos personales, máxime cuando estos son sensibles. En otras palabras, en el país si bien existe una normativa que permita indicar los lineamientos para el tratamiento de datos, falta eficacia y debido control para el cumplimiento de la misma, además, no hay claridad respecto a las excepciones, los mecanismos de control, las sanciones concretas en caso de fallas en el tratamiento de datos sensibles, acciones como indemnización, entre otros aspectos.

Paralelo a lo anterior, se encontró que la protección de los datos sensibles está relacionada directamente con la intimidad, el buen nombre y el libre desarrollo de la personalidad de los colombianos. Este es un derecho autónomo, inmerso en sus propias garantías y es reclamable por medio de la tutela. No obstante, el mal tratamiento de datos sensibles puede afectar no solo derecho a la intimidad, privacidad, buen nombre, dignidad, sino bienes jurídicos como derecho a la vida, a la salud, a la educación y al trabajo. Esto se debe a que se pueden vulnerar diversas esferas del individuo, entre ellas, la social, política y laboral.

Precisamente por los daños antijurídicos materiales e inmateriales que pueden traer sobre los titulares de los datos, el mal manejo de datos sensibles, es de gran relevancia comenzar a generar normativa que permita la tasación de dichos daños y, por tanto, los montos de indemnización y las sanciones que deben asignárseles a los tenedores de los datos. No se trata solo de imponer multas, sino de generar procesos de reparación integral cuando se le ha generado un daño grave al titular de los datos, e incluso, a sus familias.

Otra de las conclusiones a las cuales se ella es que no hay procedimientos específicos para salvaguardar los derechos de los titulares de datos personales sensibles en Colombia, al menos no de forma legal. No obstante, al revisar la literatura académica, se identifica que una estrategia que debería ser incluida por todas y cada una de las empresas que son tenedoras de datos es que estas desarrollen una acción pedagógica con sus clientes cuando estén informándoles sobre la autorización del tratamiento de datos personales, sus derechos a la corrección o eliminación de datos. Es necesario que a los titulares de los datos les quede totalmente claro que puede hacer la empresa con sus datos, hasta que punto puede usarlos y cual es el tiempo límite en que los puede tener, de este modo, el cliente, puede tomar decisiones informadas frente al tema.

Para que las empresas colombianas salvaguarden los derechos de los titulares de datos personales sensibles en Colombia, además de cumplir con los elementos trazados en la Ley 1581 de 2012 y el Decreto Único Reglamentario 1074 de 2015, los tenedores de los datos deben llevar un registro de las actividades de tratamiento de los datos sensibles, realizar periódicamente una evaluación de impacto frente al tratamiento de estos datos, incrementar acciones de transparencia, designar un colaborador que se encargue específicamente de la protección de datos sensibles, además, notificar de manera oportuna en caso de que se vulnere la seguridad de los datos sensibles en la organización.

De igual modo, se identifica que las empresas al momento de diseñar sus políticas de tratamiento de datos sensibles, deben incorporar de forma transversal los principios de privacidad, seguridad y ética. El principio de privacidad permitirá a la compañía generar acciones preventivas que le permitan evitar vulneraciones a los datos sensibles, estas acciones se asocian

al principio de seguridad, a partir del cual se busca que las empresas desarrollan acciones desde el nivel tecnológico, humano o procedimental, dirigidas a garantizar el correcto tratamiento de datos sensibles. Finalmente, la ética debe ser inherente al tratamiento de los datos desde la fase inicial referida a la recolección previa autorización, hasta la fase final en donde culmina la autorización para el tratamiento de los datos, bien sea por temporalidad o por solicitud expresa del titular de la información.

Referencias bibliográficas

Aguirre, K., Sánchez , M. (2023). P*ruebas rutinarias para el virus de inmunodeficiencia humana, y su relación con el diagnóstico clínico oportuno*. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, 5(3), 220–236.

Arboleda, W. Anaya, R. (2018). Un Acercamiento a datos abiertos en salud y su estado actual en Colombia. Pensamiento Americano. 11().

Arboleda, C. (2018). Guía para un buen manejo de datos en Colombia. Disponible en: https://www.bancolombia.com/negocios/actualizate/legal-y-tributario/guia-para-manejo-de-datos-en-colombia

Bautista-Avellaneda, M. E. (2015). Marco legal en Colombia, la Ley Estatutaria de Protección de Datos y el tratamiento penal. En: M. E. Bautista-Avellaneda. El derecho a la intimidad y su disponibilidad pública (pp. 41-51). Bogotá: Universidad Católica de Colombia

Botero, A. (2003). La metodología documental en la investigación jurídica: alcances y perspectivas. *Opinión Jurídica*. 2(4). 109-116

Caballero, J. (2015). La titularidad de los datos personales frente al concepto de persona en el ordenamiento jurídico colombiano. Disponible en: https://red.uexternado.edu.co/la-titularidad-de-los-datos-personales-frente-al-concepto-de-persona-en-el-ordenamiento-juridico-colombiano

Cano, I. (2010). Los datos religiosos en el marco del tratamiento jurídico de los datos de carácter personal. Disponible en: https://dialnet.unirioja.es/servlet/tesis?codigo=88743

Chirix, E. Sajbin, V. (2019). Estudio sobre racismo, discriminación y brechas de desigualdad en Guatemala: Una mirada conceptual. Disponible en:

https://repositorio.cepal.org/server/api/core/bitstreams/8e1d3619-36cf-44ba-bb0e-083ab0548f26/content

Corte Constitucional (2011). Sentencia C-748. MP. Jorge Ignacio Pretelt.

Corte Constitucional (2018). Sentencia T-114. MP. Carlos Bernal Pulido.

Corte Constitucional (2021). Sentencias SU139 de 21. MP. Jorge Enrique Ibáñez Najar

Corte Constitucional (2022) Sentencia T-450. MP. Jorge Enrique Ibáñez Najar

Cuartas, E. Jaller, j. (2014). El habeas data como derecho fundamental y la ley 1581 de 2012 y su decreto 1377 de 2013. [tesis]. Universidad EAFIT, Medellín

De Val, A. (2020). la protección de datos personales en los procesos de selección de los trabajadores; en particular, aquellos datos especialmente sensibles. Doc. Labor 119(1). 99 – 123

Domínguez, J. (2020). La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al covid-19. Revista de Comunicación y Salud, 10(2). 607-624

Dulzaides, M. Molina, A. (2004). Análisis documental y de información: dos componentes de un mismo proceso. *ACIMED*, 12(2), 1.

Escuela de privacidad. (2019). Sanciones por violación del Régimen de Protección de Datos Personales. Disponible en: https://escueladeprivacidad.co/2019/09/25/sanciones-por-violacion-del-regimen-de-proteccion-de-datos-personales-2019-3ra-entrega/

Fallada, J. (2012). Las políticas del racismo. Eficiencia y discriminación racial. [Tesis]. Universitat Rovira I Virgili. Tarragona, España.

Figueroa, D. Pérez, M. (2020). Decisiones de Carácter Sancionatorio Proferidas por la Superintendencia de Industria y Comercio para la Protección de los Datos Personales en Colombia entre los Años 2014 y 2019. [Tesis]. Universidad Antonio Nariño, Bogotá.

Gallo, O. (2022). Los límites de la protección a la salud de los trabajadores en Colombia, 1915-1946. *Revista Americana de Historia Social*, 21().150-172.

Galvis, A. (2012). Protección de datos en Colombia, avances y retos. Revista LEBRET, 5(4): 195-214.

García. RM.(2019). Tratamiento de datos personales de las opiniones políticas en el marco electoral: todo en interés público. 183(). 129-159.

Guzmán, D. (2016). El contexto actual del derecho a la imagen en Colombia. *Rev. Prop. Inmaterial* 47(21).

Hernández, N. (2017). Clasificación de los datos personales e implicaciones Legales. [TESIS]. Universidad Pontifica Bolivariana. Medellín, Colombia.

Key M y col. (2021). Secreto, anonimato y confidencialidad de los donantes de sangre con VIH. *Rev. Bioét. , 29*(2)(https://doi.org/10.1590/1983-80422021292466).

Ley estatutaria 1581 de 2012. or la cual se dictan disposiciones generales para la protección de datos personales. Octubre 17 de 2012.

López, D. Farriols, A. Hormazábal, H. (2019). La opinión política, un dato especialmente protegido. https://www.eldiario.es/opinion/tribuna-abierta/opinion-politica-dato-especialmente-protegido_129_1641695.html

López, S. (2011). Delimitación de la protección civil del derecho al honor, a la intimidad y a la propia imagen. Revista de Derecho UNED, 9, 43-59

Mendoza, O. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios: desafíos y cumplimiento. *Revista IUS,* 12(41). pp. 267-291

Meraz Espinoza, A. I., (2018). Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales. IUS. *Revista del Instituto de Ciencias Jurídicas de Puebla* A.C., 12(41),293-310.

Mercader, J. Puebla, A. (2018). Protección de datos y relaciones colectivas. *RTSS.CEF*, 423(1). 63-102

Monsalve, V. (2017). La protección de datos de carácter personal en los contratos electrónicos con consumidores: análisis de la legislación colombiana y de los principales referentes europeos. Prolegómenos 20(39).

Murillo, P. (2022). El racismo y la discriminación racial en Colombia. Disponible en : https://razonpublica.com/categoria/temas/politica-y-gobierno/

Newman, V. (2015). Datos personales en información pública. https://www.dejusticia.org/wp-content/uploads/2017/04/fi_name_recurso_699.pdf

Nizama, M. Nizama, L. (2020). El enfoque cualitativo en la investigación jurídica, proyecto de investigación cualitativa y seminario de tesis. VOX JURIS. 38 (2): 69-90. DOI: https://doi.org/10.24265/voxjuris.2020.v38n2.0

Ordoñez, L. (2019). El procedimiento de solicitud de adecuación de los datos de conformidad con la identidad de género. Reflexiones desde el derecho fundamental a la protección de datos. *FORO: Revista de Derecho.* 32(). 179-198

Outomuro, D. Mirabile, L. (2012). Derecho a la intimidad y su vinculación con la salud. *Revista Latinoamericana de Bioética* , 12 (1), 80-87

Pelayo, J. (2019). Retos y desafíos en la protección de datos personales que revelan las convicciones religiosas. Propuestas en un nuevo marco jurídico. Anuario de Derecho Eclesiástico del Estado, 35(). 269-350.

Peña, T. ; Pirela, J (2007). La complejidad del análisis documental. *Información, cultura y sociedad: revista del Instituto de Investigaciones*. 16(1). 55-81

Peñarete, JE & Oviedo, MP (2020). La normatividad en el tratamiento de los datos sensibles de la historia clínica, en el ejercicio del derecho del Habeas Data en Colombia. Disponible en http://hdl.handle.net/10654/35812.

Quiroz, R. (2016). El habeas data, protección al derecho a la información y a la autodeterminación informativa. Letras, 87(126), 23-49.

Quiroz, R. (2016). El habeas data, protección al derecho a la información y a la autodeterminación informativa. Letras, 87(126), 23-49.

Rivera, W. (2007). Investigación jurídica. https://issuu.com/unebiblioteca/docs/investigacion_juridica

Rodríguez, J. (2008). La protección de los datos personales y las confesiones religiosas. Laicidad y Libertades. 8().329- 370

Rojas, 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*, 8(1), 107-139.

Rojas, 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, 8(1), 107-139.

Salvador, V. (2017). El futuro marco legal para la protección del acceso a los datos. Revista Ibero-Latinoamericana de Seguros, 26(47).

Sánchez, M. (2021). La Protección y el tratamiento de datos personales. El derecho humano a la privacidad y a la intimidad. Mirada Legislativa. 201(). 1-24.

Superintendencia de Industria y Comercio. (2019). Sanciones por violación del Régimen de Protección de Datos Personales 2019. Disponible en: https://escueladeprivacidad.co/2019/09/25/sanciones-por-violacion-del-regimen-de-proteccion-de-datos-personales-2019-3ra-entrega/

Superintendencia de Industria y Comercio. (2022). Lo que se podrá o no hacer con datos personales durante elecciones. https://www.portafolio.co/economia/gobierno/reglas-de-juego-para-tratamiento-de-datos-personales-en-elecciones-560713

Tantaleán, A. (2016). El alcance de las investigaciones jurídicas. *Derecho y Cambio Social*. 1-22.

Valencia, J. Marín, S. (2018). Investigación teórica, dogmática, hermenéutica, doctrinal y empírica de las ciencias jurídicas. *Ratio Juris. 13*(27).17-26

Villabella, C. (2015). Los métodos en la investigación jurídica. https://archivos.juridicas.unam.mx/www/bjv/libros/8/3983/46.pdf

Viveros, M. (2007). Discriminación racial, intervención social y subjetividad. *Revista de Estudios Sociales*. 27(230). 106-121