Revista CIES – ISSN-e 2216-0167. Volumen 12. Número 2. Año 2021. Páginas 303-313. Dirección de Investigaciones – Institución Universitaria Escolme (Medellín, Colombia)

Protección de los datos personales en los servicios de internet y las aplicaciones en Colombia

Ronal Santiago Colorado Restrepo
Tecnología en Redes y Seguridad Informática, Institución Universitaria Escolme, Medellín, Colombia, rscolorador@escolme.edu.co

Recibido: 14/9/2021 - **Aceptado:** 5/10/2021 - **Publicado:** 21/10/2021

RESUMEN

En la actualidad con la llegada de las nuevas tendencias derivadas de la práctica internacional de la información, resulta relevante atender las necesidades de la visión global de la misma, lo cual ha implicado la creación de nuevos escenarios legales con el fin de dar solución ágil a las relaciones informáticas; por lo cual los diferentes actores de naturaleza privada y pública han orientado importantes esfuerzos para lograr los objetivos de proteger la información al interior de sus diferentes corporaciones, adquiriendo en gran medida diversidad de beneficios en materia de información. Por lo anterior, se propone como objetivo describir la situación actual del cumplimiento a la protección de los datos personales qué se suministran en los servicios de internet y las aplicaciones en Colombia. Se desarrolló una investigación cualitativa documental, se revisaron 39 fuentes de información formal e informal. Se evidenció interés estatal por la regulación de procesos relacionados con la protección de datos, sin embargo, hay una tendencia hacia el aumento de la violación de este derecho.

Palabras clave: Protección de datos; TIC; Seguridad Informática.

ABSTRACT

At present, with the arrival of new trends derived from the international practice of information, it is relevant to meet the needs of the global vision of the same, which has implied the creation of new legal scenarios in order to provide an agile solution to computer relationships; For this reason, the different actors of a private and public nature have directed important efforts to achieve the objectives of protecting information within their different corporations, acquiring to a great extent diversity of benefits in terms of information. Therefore, it is proposed as an objective to describe the current situation of compliance with the protection of personal data that is provided in internet services and applications in Colombia. A qualitative documentary research was developed, 39 formal and informal sources of information were reviewed. There is evidence of state interest in the regulation of processes related to data protection, however, there is a trend towards an increase in the violation of this right.

Keywords: Data Protection; ICT; Information Security.

1. INTRODUCCIÓN

Diariamente los ciudadanos colombianos exponen su información en internet para hacer uso de herramientas del día a día como lo son redes sociales y correo electrónico, entre otras; esto representa un riesgo para su información ya que pese a aceptar las condiciones de uso de estos servicios, se ignora la realidad de las políticas aceptadas, y el uso que los propietarios de estas herramientas le están dando a lo recolectado (Castro-Jaramillo, Guevara-Valencia & Jaramillo-Rojas, 2016).

Normalmente los servidores de estos servicios se encuentran en diferentes países, por lo que es complejo determinar las leyes, variantes y sanciones reglamentadas para la protección de la información; por lo anterior es importante dar una mirada reflexiva al buen uso de los datos personales que Colombia ha regulado y su cumplimiento cuando se abordan nuevos escenarios como el ciberespacio (Ministerio de Tecnologías de la Información y las Comunicaciones de la República de Colombia [MINTIC], s.f.).

En concordancia con la ley de protección de datos personales y los temas concernientes a seguridad de la información de cada uno de los ciudadanos colombianos, es necesario analizar cuáles son las políticas de tratamiento de datos o "términos y condiciones de uso" que los proveedores de servicios en internet están poniendo a disposición de sus usuarios y su alineación con las disposiciones que Colombia ha regulado al respecto (Castro, 2016, Bermeo-Giraldo et al., 2020).

El despliegue de tecnologías de la información y la comunicación (TIC) generalizadas dentro de las iniciativas de ciudades inteligentes transforma las ciudades en extraordinarios aparatos de captura de datos (Galič & Gellert, 2021; Valencia-Arias, Urrego-Marín & Bran-Piedrahita, 2021). En la actualidad, con las crecientes necesidades del mundo globalizado y las nuevas tendencias de la híper-conexión, el Estado colombiano se vio en la necesidad de expedir diferentes reglamentaciones que permitieran dar regulación a la información personal generada en estas plataformas, como lo son: la Ley 1266 de 2008 sobre habeas data y la Ley 1581 de 2012 sobre protección de datos personales, con las cuales se pretende regular la totalidad de las actividades de tratamiento de datos de la población colombiana (Ley Estatutaria 1266, 2008; Ley Estatutaria 1581, 2012).

Sin embargo, la realidad actual después de seis años de expedición legal, radica en no evidenciar la estandarización del Estado colombiano a las necesidades internacionales, e incluso catalogan a Colombia como un país que no cuenta con un nivel adecuado de protección de datos, ejemplo de ello se encuentra la negativa a Colombia de la declaración de nivel de protección adecuado de la Comisión Europea, la cual en la actualidad representa ser el marco legal pionero en protección de datos, al brindar el mayor nivel de garantía a sus asociados (Guzmán, 2015).

Es así que se hace necesario materializar la presente investigación, encaminada a describir la situación actual del cumplimiento a la protección de los datos personales qué se suministran en los servicios de internet y las aplicaciones en Colombia mediante un estudio que permita conocer las políticas y lineamientos existentes para la seguridad de la información en el tratamiento y confidencialidad de los datos personales.

2. MARCO TEÓRICO Y/O ANTECEDENTES

El conocimiento sobre los derechos que tienen los ciudadanos y las empresas en relación con el manejo de sus datos personales es un área que requiere mucha atención, para saber cómo y en qué momento autorizar su uso por parte de terceros. Colombia tiene un marco regulatorio bastante robusto en relación con los datos personales, está enmarcado en la constitución.

En el contexto colombiano está fundamentado jurídicamente sobre desarrollos constitucionales, legales y administrativos, que se articulan y cobran forma en la competencia de la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio (en adelante DPD-SIC), la cual fue consagrada como la Autoridad de Protección de Datos en Colombia (en adelante APD). Este sistema surge del artículo 15 de la Constitución Política de 1991, que reconoce el derecho de las personas a la intimidad personal, al buen nombre, a la inviolabilidad de la correspondencia, y al habeas data, consistente en el derecho de conocer, actualizar y rectificar la información personal que haya sido colectada en bases de datos públicas o privadas (Superintendencia de Industria y Comercio, 2018).

El habeas data tuvo regulación y definición legal mediante la Ley 1266 de 2008, que está dirigida a definir la PDP en materia de información de carácter financiero, comercial, de servicios y proveniente de terceros países, destinada al cálculo del riesgo crediticio, haciendo de esta una regulación restringida, sectorial y especial (Ley Estatutaria 1266, 2008).

Con la expedición de la Ley Estatutaria 1581 de 2012, el Departamento Nacional de Planeación y el Ministerio de Tecnologías de la Información y las Comunicaciones, liderarán la implementación de la política nacional de explotación de datos (Big Data), en un periodo de implementación de cinco años, con inversiones por 16.728 millones de pesos para la creación de las condiciones descritas, para adecuar la intervención pública y orientarla a la generación de valor, con los datos se instituyó una cobertura general más amplia de la PDP que trascendió a otros tipos de información, incorporando además definiciones fundamentales que pusieron el régimen colombiano de PDP a tono con las mejores prácticas internacionales documentadas de su momento (Consejo Nacional de Política Económica y Social [CONPES], 2018).

A ello se suman el decreto 1377 de 2013, que reglamenta la Ley 1581, y el Título V de la Circular Única de la Superintendencia de Industria y Comercio, como instrumentos jurídicos principales de regulación y aplicación directa. Haciendo una revisión detallada de los pronunciamientos de la DPD-SIC en su ejercicio como APD, se observa que esta ha tomado a la fecha 58 decisiones con las que se determinó la responsabilidad por algún tipo de vulneración de la PDP en cada una de ellas. De estas, tan solo 6 decisiones (10,3%) no condujeron a sanción económica, mientras que las otras 52 suman un total de 1,6 millones de dólares en multas a los responsables, impuestas en un lapso de 4 años (Superintendencia de Industria y Comercio, 2018).

El 32,8% de los casos implicó vulneración al deber de conservar la información bajo condiciones óptimas de seguridad, de modo que los datos personales terminaron al alcance

de terceros no autorizados. En el 55,2% se encontraron fallas en el cumplimiento de la autorización del titular para hacer el tratamiento de datos, ya fuera porque no había autorización, o porque la había, pero no se informó la finalidad de los datos, o porque se informó, pero se dio un uso distinto. Y en el 58,6% se halló una vulneración directa al habeas data, ya fuera porque no había un canal para acudir al responsable de los datos, o porque existía el canal, pero no se atendió la solicitud del titular, o porque se atendió la solicitud, pero no se resolvió de fondo el motivo de la solicitud. Además, se encontró que en el 13,8% de los casos el responsable no contaba con políticas para el tratamiento de la información, o contaba con ellas, pero no estaban al acceso de los titulares (Superintendencia de Industria y Comercio, 2018).

Se encuentra además que los responsables por el incumplimiento al régimen de PDP son sumamente variados, encontrando compañías de comercio electrónico, empresas de servicios públicos, instituciones educativas, prestadores de servicios de salud, hoteles, centros comerciales, editoriales, candidatos políticos, etc. Los casos más representativos son el de Casa Editorial El Tiempo S.A. y Linio S.A.S, las más sancionadas con 4 anotaciones para cada una, todas ellas por vulneración del habeas data. Un caso particular que llama la atención de la superintendencia de industria y comercio (Superintendencia de Industria y Comercio, 2018).

Esto es una muestra de que en Colombia existen empresas que no tienen conocimiento pleno de sus obligaciones frente a la PDP, y por su desconocimiento están vulnerando el derecho fundamental del habeas data. Así mismo, las personas están acudiendo cada vez más a la DPD-SIC a denunciar estos hechos, lo que se traduce en más decisiones y más sanciones (7 casos en 2015 Vs 16 casos en 2017). Es la muestra de la conciencia que tiene la ciudadanía respecto de la PDP. Colombia está asumiendo innovaciones y actualizaciones necesarias frente a la relación entre el Big Data, la PDP, y el entorno globalizado en el que fluye la información al mismo tiempo, existe una iniciativa parlamentaria para actualizar el régimen general de PDP, asesorada por el Observatorio Ciro Angarita Barón sobre Protección de Datos en Colombia, que busca proveer a la APD de mayores herramientas para perseguir las vulneraciones del habeas data cometidas por corporaciones en un contexto internacional tal como la documentada en el caso de Facebook (CONPES, 2018).

Hoy día es muy común en las estrategias de relacionamiento de los diferentes sectores de la economía utilizar el sistema de correo electrónico masivo, contacto por medio de referidos, estudio de mercados por minería de datos, big data, etc., pero para ello es necesario contar con Políticas de Tratamiento de Datos, lo que implica la definición de aspectos tales como la forma de recolección de datos personales y la autorización de los titulares para su uso de acuerdo a una finalidades previamente establecidas. Así mismo dentro de dichas políticas se debe establecer todo el trámite administrativo de almacenamiento, tratamiento, procesamiento, intercambio y procesos para las consultas y trámites de quejas. Todo ello redundará en la garantía del tratamiento de los datos de las personas y en la disminución de la vulneración de derechos fundamentales y de los volúmenes de quejas y reclamos por el tratamiento de datos personales no autorizados (Buitrago, 2016).

3. METODOLOGÍA O DESCRIPCIÓN DEL PROCESO

Se desarrolla una investigación documental, la cual es una técnica cualitativa que se encarga de recopilar y seleccionar información a través de la lectura de documentos, libros, revistas.

De igual forma, se considera de tipo informativa dado que busca describir la situación actual del cumplimiento a la protección de los datos personales qué se suministran en los servicios de internet y las aplicaciones en Colombia.

Para la revisión documental se definieron unos criterios de la información a utilizar:

1. Actualidad: Para conocer la magnitud del problema se exportaron citas actuales de fuentes oficiales, también se describe el marco normativo y las estrategias que utiliza el país para afrontar las dificultades en torno a la protección de los datos personales
2. Pertinencia: Que la información a utilizar guardará una estrecha relación con el tema de estudio y que estuviese aplicado al contexto colombiano.
3. Canal de la información: Se utilizaron fuentes como formales e informales para dar respuesta al objeto de estudio. Como formales se reconoces, tesis, libros, documentos oficiales e informales como conferencias, entrevistas publicadas, noticias de medios de reconocidos.

4. ANÁLISIS DE RESULTADOS O HALLAZGOS

Según la Superintendencia de Industria y Comercio-SIC, actualmente, un gran número de empresas pueden tener acceso la información de las personas, información que suele ser obtenida mediante estrategias de marketing fuertes. Entre 2017 y 2019, las multas más altas que ha impartido SIC han sido por violación a la normativa de protección de datos personales, costos que ascienden a más de 21 mil millones de pesos cada año (Casanova et al., 2020).

De acuerdo con la información suministrada por la SIC, alrededor del 80% de las sanciones impuestas por esta entidad se relacionan con infracciones al Habeas Data financiero, las causas son: la no actualización oportuna de la información, los reportes a centrales de riesgos que no corresponden a la realidad y la falta de notificación al deudor antes de realizar el reporte a las centrales de riesgo, entre otros (Superintendencia de Industria y Comercio, 2017**)**.

En Colombia, según la SIC durante 2019 se recibieron 12.741 denuncias por los usuarios dado un mal tratamiento de esta información por parte de terceros. La cifra, que es la más alta registrada en un año, significa un crecimiento de 36,01% frente al 2018 (Superintendencia de Industria y Comercio, 2020).

Adicionalmente, durante el año 2020 la SIC, también informa que se impusieron multas por $7.580.187.680, y se emitieron 2.070 órdenes para que las empresas cumplan con la legislación que protege los datos personales. Dado la magnitud de las denuncias frente a la violación de datos personales la SIC ha creado unas guías para facilitar el cumplimiento de las normas regulatorias para la temática en mención (Superintendencia de Industria y Comercio, 2021). Algunas de ellas son:

Tabla 1. Guía para el correcto tratamiento de datos

Guía	Objeto
Gestión de incidentes de seguridad	Esta guía tiene como propósito presentar algunas sugerencias a los Responsables y los Encargados del Tratamiento de Datos Personales, con miras a orientarlos para que cuenten con un plan dirigido a afrontar los incidentes de seguridad que afecten los Datos Personales bajo su custodia o posesión. Cualquier acción en este sentido debe centrarse en mitigar su impacto sobre los Titulares de la información y sus datos. Algunos puntos que considera relevante la guía son capacitar a los miembros, dar instrucciones claras, definir cláusulas de confidencialidad.
Fotos como datos personales	Esta guía tiene como propósito presentar algunas sugerencias a los Responsables y Encargados del Tratamiento de fotos con miras a orientarlos para que no incurran en ninguna irregularidad respecto de la regulación sobre el Tratamiento de Datos Personales. Tiene un enfoque preventivo con miras a que una empresa directamente (Responsable del Tratamiento) o a través de terceros (Encargado del Tratamiento) evite vulnerar los derechos de cualquier persona o cliente (Titular del Dato).
Tratamiento de datos en la propiedad horizontal	Esta guía tiene como propósito presentar algunas sugerencias a quienes recolectan o tratan Datos Personales en los edificios o conjuntos de uso residencial, comercial o mixto sometidos al régimen de propiedad horizontal, con miras a orientarlos para que cumplan correctamente la regulación sobre el Tratamiento de los mismos y, de esta manera, respeten los derechos de las personas
Guía sobre el Tratamiento de Datos Personales para fines de comercio electrónico	El comercio electrónico es el motor de la economía del siglo XXI y los datos personales son la moneda de la economía digital, es una fuerte estrategia para ampliar el mercado y comercializar productos o servicios. Dentro de las recomendaciones que da la guía , están aquellas acciones relacionadas con: Exigir el respeto de la Política de Tratamiento de Datos Personales a los terceros que contrata para realizar actividades de comercio electrónico, efectuar estudios de impacto de IV privacidad, evitar la suplantación de identidad de los consumidores
Guía sobre el Tratamiento de Datos Personales para fines de marketing y publicidad	Presentar algunas sugerencias a quienes utilizan datos personales para realizar actividades de marketing, publicidad y mercadotecnia con el fin de orientarlos para que desde el diseño de cualquier gestión o campaña publicitaria tenga en cuenta las exigencias de las regulaciones sobre Tratamiento de Datos Personales (TDP).

Fuente: Superintendencia de Industria y Comercio (2021).

El correcto cumplimiento de la norma de protección de datos y con el propósito de salvaguardar el activo más importante que es la información; es necesario tener en cuenta

que la empresa debe contar con un sistema de administración de los riesgos asociados al tratamiento de datos personales, el cual debe contar con elementos de: identificación, medición, control y monitoreo, que junto a las medidas técnicas de seguridad, controles, capacitación y comunicación interna y externa, permitan conformar un Programa Integral de Gestión de Datos Personales y Seguridad de la Información.

Por lo anterior, se brindan una serie de recomendaciones relacionadas con el manejo de los datos personales:

Tabla 2. Recomendaciones para el manejo de los datos personales

Criterio	Descripción
Proteger su información personal fuera de internet	Guarde bien su información y manténgala fuera del alcance de las personas con quien comparte en su casa, oficina, lugar de trabajo, guarde todos sus documentos y registros financieros bajo llave y en un lugar seguro de su casa (IFORENSEColombia, 2019).
Proteger su información personal en internet	No suministre información personal por teléfono, por correo electrónico, ni en internet, a menos que usted haya iniciado el contacto o sepa con quién está tratando. Si recibe un email de una compañía que aduce tener una cuenta con usted y le piden información personal, no haga clic sobre ningún enlace electrónico del email, verifique el nombre de la compañía que le envió el correo en su navegador de internet, vaya a ese sitio y comuníquese con la compañía a través del servicio al cliente. O llame al número de teléfono del servicio al cliente que aparece listado en su resumen de cuenta. Pregunte si la compañía envió ese email solicitándole la información (IFORENSEColombia, 2019).
Elimine la información personal de manera segura	Elimine toda la información almacenada. Use un programa de barrido para sobrescribir y limpiar todo el disco duro o medio donde conserva la información (IFORENSEColombia, 2019).
Encripte sus dato	Controle la seguridad de su navegador de internet, utilice el modo incognito, use un programa de encriptación que cifre los datos enviados por internet, elimine los historiales de búsquedas, siempre utilice fuentes confiables para realizar descargas (IFORENSEColombia, 2019).
No comparta sus contraseñas con nadie	Utilice siempre contraseñas sólidas para su computadora portátil y para acceder a sus cuentas de crédito, bancarias y demás cuentas. Siempre utilice contraseñas alfanuméricas, utilice letras mayúsculas y minúsculas con longitudes largas (IFORENSEColombia, 2019).
No comparta demasiada información en los sitios de redes sociales	Establecer límites para que sólo un pequeño grupo de personas pueda acceder a su página de redes sociales, nunca divulgue su nombre completo, lugar de residencia, número de teléfono o números de cuenta en sitios de acceso libre al público. (IFORENSEColombia, 2019).

Proteja su computadora y aparatos móviles	Instale programas antivirus y anti-espía, y un firewall, configure las preferencias de los programas para que las protecciones se actualicen frecuentemente, proteja su computadora y los dispositivos contra intrusiones e infecciones que pueden poner en riesgo los archivos o sus contraseñas instalando los parches de seguridad ofrecidos por su sistema operativo y otros programas (IFORENSEColombia, 2019).
Lea las políticas de privacidad	Las políticas pueden ser extensas y complejas, pero el texto de la política de privacidad de cada sitio le informará cómo se mantiene la exactitud, acceso, seguridad y control de la información personal que recolecta; cómo se usa la información, y si provee información a terceros, si no encuentra o no entiende la política de privacidad de un sitio web, considere hacer las actividades en otra parte (IFORENSEColombia, 2019).
Brindar datos personales sólo en sitios de confianza	Muchas páginas piden datos personales, antes de dárselos es importante que te asegures que no sea un sitio web falso, qué datos necesitan y para qué los van a utilizar, además, revisa que la web que te solicita la información cuente con el protocolo SSL (Secure Sockets Layer), es decir, que la dirección que aparece en el navegador inicie con HTTPS. Esto permite que los datos que compartiste viajen por un canal cifrado (Microsip, s.f.).
Descarga archivos y aplicaciones únicamente de sitios reconocidos	Existen muchos sitios web de descarga gratuita de programas que engañan a los usuarios para obtener datos y acceso a tu computadora, y al descargar la aplicación se ejecutan de forma oculta contenidos maliciosos que destruyen o que se apropian de los datos almacenados, como números de tarjetas, número de seguro social, contraseñas, correos electrónicos, entre otros. Para evitar esta situación, navega y descarga únicamente contenidos de sitios de confianza (Microsip, s.f.).
Evita conectarte a redes públicas:	Muchos lugares ofrecen acceso gratuito a Wi-Fi, pero por más tentador que sea, ten cuidado, no sabes quién puede acceder a tus dispositivos ni cuáles son las medidas de seguridad que posee, si aun así decides conectarte, nunca ingreses datos privados ni accedas a servicios bancarios, correo electrónico y redes sociales (Microsip, s.f.).
Vigilar las aplicaciones que se conectan con los perfiles en redes sociales	En las redes sociales, existen multitud de juegos y aplicaciones que son desarrolladas por terceras personas, y para utilizarlas, el usuario debe aceptar ciertas condiciones y permisos de acceso a su perfil. Suele suceder que muy pocos leen en detalle lo que implica la descarga sin tener en cuenta que podría estar brindando acceso a sus datos personales a través de la aplicación como acceso a fotografías, correo electrónico, información de nuestros contactos, etc. (AltoDirectivo, 2019).

Utiliza la Doble verificación	En el caso de ser atacado y el pirata sepa la clave no podrá entrar porque es necesario el código que has recibido en el móvil (Beck Destrucción Confidencial, s.f.).

Fuente: IFORENSEColombia (2019); Microsip (s.f.); AltoDirectivo (2019); Beck Destrucción Confidencial (s.f.).

5. CONCLUSIONES

Con la implementación de las TIC, cada vez más es posible recolectar datos de personales, pero a su vez a un gran riesgo en su manejo. Este riesgo ha generado que desde contextos internacionales y nacionales se regulen políticas para proteger de los datos de los individuos. Pese a ello, aun el país se presenta un alto volumen de vulneración a este derecho. De igual forma, en la sociedad existe un bajo empoderamiento frente a la importancia de esta acción.

6. REFERENCIAS

AltoDirectivo. (2019). Siete consejos para proteger mis datos en las redes sociales Recuperado de http://www.altodirectivo.com/secciones/25655/siete-consejos-para-proteger-mis-datos-en-las-redes-sociales

Beck Destrucción Confidencial. (s.f.). ¿Cómo mejorar nuestra protección de datos en internet? Recuperado de https://abdc.es/blog/mejorar-proteccion-de-datos-personales-en-internet/

Bermeo-Giraldo, M. C., Valencia-Arias, A., Garcés, L. F., & García, D. A. (2020). Principales tendencias investigativas en seguridad de redes informáticas a partir del estudio bibliométrico de la literatura desde 1973 al 2019. En Sepúlveda, J. A (Ed.), *Evolución y tendencias investigativas en Ingeniería de Sistemas e Ingeniería Industrial* (pp. 52-81). Medellín, Colombia: Sello Editorial Coruniamericana.

Buitrago, D. M. (2016). Editorial - El valor de los datos personales en Colombia. *Revista CES, 7*(1), 1-2. Recuperado de http://www.scielo.org.co/pdf/cesd/v7n1/v7n1a01.pdf

Casanova, C., Correa, M. J., Morales, O., Acosta, M., & Rojas, A. (15 de Septiembre de 2020). Habeas Data: una lucha continua de la SIC. Recuperado de https://plataforma.bucaramanga.upb.edu.co/acontecer/habeas-data-una-lucha-continua-de-la-sic

Castro, Á. M. (2016). Derecho a la intimidad en las redes sociales de internet en Colombia. *Novum Jus: Revista Especializada en Sociología Jurídica y Política, 10*(1), 113-133. Recuperado de https://novumjus.ucatolica.edu.co/article/view/1178/1165

Castro-Jaramillo, Á., Guevara-Valencia, S., & Jaramillo-Rojas, C. (2016). Análisis sociojurídico del surgimiento y expansión de las redes sociales en internet y la intimidad en Colombia. *Criterio Libre Jurídico, 13*(2), 67-78. https://doi.org/10.18041/crilibjur.2016.v13n2.26201

Consejo Nacional de Política Económica y Social – CONPES. (17 de abril de 2018). Política nacional de explotación de datos (Big Data). Recuperado de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3920.pdf

El Congreso de Colombia. (31 de diciembre de 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. [Ley Estatutaria 1266 de 2008]. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

El Congreso de Colombia. (17 de octubre de 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. [Ley Estatutaria 1581 de 2012]. Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

Galič, M., & Gellert, R. (2021). Data protection law beyond identifiability? Atmospheric profiles, nudging and the Stratumseind Living Lab. *Computer Law & Security Review, 40*, 1-13. https://doi.org/10.1016/j.clsr.2020.105486

Guzmán, D. (3 de septiembre de 2015). Derecho de imagen en la ley de protección de datos personales. Recuperado de https://propintel.uexternado.edu.co/derecho-de-imagen-en-la-ley-de-proteccion-de-datos-personales/

IFORENSEColombia. (2019). Cómo proteger mi información personal. Recuperado de https://www.informaticaforense.com.co/como-proteger-mi-informacion-personal/

Microsip. (s.f.). Protección de tus datos personales: 9 medidas de seguridad. Recuperado de https://blog.microsip.com/9-medidas-para-proteger-tus-datos-personales/

Ministerio de Tecnologías de la Información y las Comunicaciones de la República de Colombia. (s.f.). Políticas de Privacidad y Condiciones de Uso. Recuperado de https://www.mintic.gov.co/portal/inicio/2627:Pol-ticas-de-Privacidad-y-Condiciones-de-Uso

Superintendencia de Industria y Comercio. (2017). Por violaciones de datos personales, Superindustria ha impuesto sanciones por más de $21 mil millones de pesos. Recuperado de https://www.sic.gov.co/noticias/por-violaciones-de-datos-personales-superindustria-ha-impuesto-sanciones-por-mas-de-21-mil-millones-de-pesos

Superintendencia de Industria y Comercio. (2018). La protección de datos personales desde la perspectiva de los estudiantes universitarios de la ciudad de Bogotá. Recuperado de https://www.sic.gov.co/sites/default/files/files/Noticias/Compilaci%C3%B3n%20Ensayos%20Protecci%C3%B3n%20Datos%20Personales%202018.pdf

Superintendencia de Industria y Comercio. (2020). Día Internacional de Protección de Datos: un llamado a las buenas prácticas. Recuperado de https://www.sic.gov.co/noticias/d%C3%ADa-internacional-de-protecci%C3%B3n-de-datos-un-llamado-las-buenas-pr%C3%A1cticas

Superintendencia de Industria y Comercio. (2021). Más de 16 mil quejas recibió la Superindustria en 2020 por protección de datos personales. Recuperado de https://www.sic.gov.co/slider/m%C3%A1s-de-16-mil-quejas-recibi%C3%B3-la-superindustria-en-2020-por-protecci%C3%B3n-de-datos-personales

Valencia-Arias, A., Urrego-Marín, M. L., & Bran-Piedrahita, L. (2021). A Methodological Model to Evaluate Smart City Sustainability. *Sustainability, 13*(20), 1-17. https://doi.org/10.3390/su132011214